SOCIAL MEDIA, WIRETAPPING, AND INTERCEPTED EVIDENCE

EMILY MISKEL
KoonsFuller, P.C.
5700 W. Plano Pkwy., Suite 2200
Plano, Texas 75093
(972) 769-2727
emily@koonsfuller.com

State Bar of Texas
40TH ANNUAL
ADVANCED CRIMINAL LAW COURSE
July 21-24, 2014
Houston

CHAPTER 48
BIOGRAPHICAL INFORMATION

EDUCATION
B.S. in Mechanical Engineering, with distinction, Stanford University
J.D., Harvard Law School

PROFESSIONAL RECOGNITION
Board Certified, Family Law — Texas Board of Legal Specialization
Young Lawyer of the Year, 2010-2011, Collin County Young Lawyers Association
2010 Leadership Class, Dallas Association of Young Lawyers
Life Fellow, Dallas Association of Young Lawyers Foundation

PROFESSIONAL AFFILIATIONS
Secretary, Harvard Club of Dallas
Board Member, Stanford Club of Dallas Ft. Worth
Henderson Inn of Court
Collaborative Law Institute of Texas
Texas Academy of Family Law Specialists (TAFLS)

RECENT PUBLICATIONS AND SPEECHES
**Complete list available at www.emilymiskel.com**
Real-World Evidence Traps, Texas A&M Law Clinic, April 2014.
Authenticating Social Media – Admissibility, Fall Judicial Education Session, Texas Judicial Academy (2013).
Property Issues in Divorce, How to do a Pro Bono Divorce, Texas Young Lawyers Association (2013).
Representing Yourself in a Divorce, a Guide from the Dallas Bar Association, Dallas Volunteer Attorney Program (2013), co-author.
Electronic Evidence Cases Every Family Lawyer Should Know, Dallas County Bar Association, Dallas County Family Law Bench Bar (2013), co-author.
Electronic Evidence, Texas Bar College Summer School, State Bar of Texas (2012).
TABLE OF CONTENTS

I. SCOPE OF ARTICLE ................................................................. 1
II. FEDERAL CLAIMS IN STATE COURT .................................................. 1
III. FEDERAL LAWS ........................................................................ 1
IV. FEDERAL WIRETAP ACT ............................................................. 2
   A. Interception ........................................................................... 2
      1. Definition ........................................................................ 2
      2. Cordless, Wireless, or Cellular Communications ............. 2
   B. Use and Disclosure ............................................................... 2
   C. Definitions ........................................................................... 2
      1. Wire Communication ....................................................... 3
      2. Oral Communication ...................................................... 3
      3. Electronic Communication ............................................. 3
   D. Penalties .............................................................................. 3
      1. Criminal .......................................................................... 3
      2. Civil ................................................................................. 3
      3. Statute of Limitations ..................................................... 4
   E. Exclusionary Rule ................................................................. 4
   F. Consent ............................................................................... 5
      1. One-Party Consent .......................................................... 5
      2. All-Party Consent ........................................................... 5
      3. No Spousal Exception ..................................................... 5
      4. Vicarious Consent .......................................................... 6

V. TEXAS STATE WIRETAPPING LAW ............................................. 6
   A. Offense ............................................................................... 6
   B. Penalties ............................................................................ 7
      1. Criminal .......................................................................... 7
      2. Civil ................................................................................. 7
      3. Damages ......................................................................... 7

VI. OVERLAP BETWEEN WIRETAP ACT AND STORED COMMUNICATIONS ACT ................................. 8
VII. FEDERAL STORED COMMUNICATIONS ACT ........................................ 8
    A. Offense ............................................................................ 8
    B. Definitions ....................................................................... 8
       1. Wire and Electronic Communications .............................. 8
       2. Electronic Storage .......................................................... 8
    C. Penalties .......................................................................... 9
       1. Criminal ........................................................................ 9
       2. Civil ............................................................................. 9
       3. Statute of Limitations ................................................. 10

VIII. TEXAS STATE STORED COMMUNICATIONS LAW ................................ 10
IX. FIRST AMENDMENT ................................................................ 10
   A. Filming Police ................................................................... 10
   B. Recording Public Figures ................................................ 11
   C. Online Threats ................................................................. 11

X. OTHER TEXAS COMPUTER CRIMES ............................................. 11
   A. Online Impersonation ....................................................... 11
   B. Breach of Computer Security ......................................... 12
   C. Civil Cause of Action ....................................................... 14

XI. CONCLUSION .......................................................................... 14

APPENDIX .................................................................................. 15
SOCIAL MEDIA, WIRETAPPING, AND INTERCEPTED EVIDENCE.

I. SCOPE OF ARTICLE.

This article will give an overview of state and federal laws relating to wiretapping and interception of data, including both criminal laws and civil causes of action. This paper focuses on the portions of the laws that are most likely to affect an attorney in private practice. There are many other sections of the laws relating to law enforcement and criminal investigations that are beyond the scope of this paper.

The federal laws are very complex and technical, often requiring fine-grained statutory interpretation to understand. It would be possible to write an entire textbook on the intricacies of these laws. This article is designed to give a brief overview of the landscape of these interlocking laws so that the practicing attorney will have a basic understanding of the framework and will have a starting point for more in-depth learning.

II. FEDERAL CLAIMS IN STATE COURT

This paper contains an extensive discussion of federal laws relating to wiretapping and data interception. These federal laws are relevant to attorneys who practice exclusively in state court because these federal claims may be brought in state court. Although it is currently rare, it would be possible to add a federal Wiretap Act civil claim to a divorce case, for example.

This stems from the United States Constitutional system of federalism, which provides that federal courts are courts of limited jurisdiction, while state courts are courts of general jurisdiction. Nothing in the concept of the federal system prevents state courts from enforcing rights created by federal law. Concurrent jurisdiction has been a common phenomenon in United States judicial history, and exclusive federal court jurisdiction over cases arising under federal law has been the exception rather than the rule. Under the federal system, the states possess sovereignty concurrent with that of the federal government, subject only to limitations imposed by the Supremacy Clause. Under this system of dual sovereignty, the U.S. Supreme Court has consistently held that state courts have inherent authority, and are thus presumptively competent, to adjudicate claims arising under the federal laws of the United States.

A state court is only precluded from hearing federal claims if Congress has given exclusive jurisdiction to federal courts. To give federal courts exclusive jurisdiction over a federal cause of action, Congress must, in an exercise of its powers under the Supremacy Clause, affirmatively divest state courts of their presumptively concurrent jurisdiction. Absent an exclusive grant of jurisdiction to the federal courts in the Congressional act, state courts of general jurisdiction have concurrent authority to adjudicate federally created causes of action.

Specifically, state courts have jurisdiction over federal wiretap claims. Nothing in the federal wiretapping act suggests that Congress confined jurisdiction solely to the federal courts. Texas courts have addressed claims under the Federal Wiretap Act.

For the reasons stated below, it will be increasingly likely to encounter these federal claims, even in a state-court practice.

III. FEDERAL LAWS

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, more commonly known as the “Wiretap Act,” is found at 18 U.S.C. §§ 2510-2522. As the name suggests, the Wiretap Act was passed in the 1960s. Although it was updated in 1986 and 1994, it can be an imperfect match for many of the modern technologies that have been created in the 20 years since its last update. Courts have held that:

the intersection of these two statutes is a complex, often convoluted, area of the law. The difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results. Until Congress brings the laws in line with modern technology, protection of the Internet will remain a confusing and uncertain area of the law.

---

2 Id.
4 Id. at 459.
The Electronic Communications Privacy Act of 1986 (ECPA) amended the Wiretap Act to include electronic data and added the Stored Communications Act, 18 U.S.C. §§ 2701-2712. Sometimes cases will refer to the wiretap laws as Title I of the ECPA and to the Stored Communications Act as Title II of the ECPA.

IV. FEDERAL WIRETAP ACT.

The Wiretap Act generally sets forth three categories of offenses: interception of communications, use of intercepted communications, and disclosure of intercepted communications. (There is a fourth category of offenses, dealing with mechanical devices or “bugs.” This paper will not address those offenses, because they are not as relevant to the general practice of the audience for this paper.) The Wiretap Act also contains a civil cause of action and a strict exclusionary rule.

A. Interception.

1. Definition.

The Wiretap Act is violated when any person:

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication.\(^{11}\)

The Wiretap Act is an extremely technical statute. Most of the words used are statutorily-defined terms which differ from the commonly-understood definitions of the words. Any time you are working with the federal statutes, it is extremely important to read and re-read the defined terms. The definitions of “wire communication,” “oral communication,” and “electronic communication” are discussed in more detail below.

2. Cordless, Wireless, or Cellular Communications.

In 1968, when the Wiretap Act was originally enacted, cordless, wireless, or cellular phones did not exist as a consumer product. Therefore, under the original act, cordless, wireless, or cellular transmissions were considered “radio transmissions” and were not protected at all against interception. Courts further held that no one could have any reasonable expectation of privacy in such conversations.\(^{12}\) Now, however, most people strongly believe that there is an expectation of privacy in cordless or wireless conversations, and in fact the Act was updated in 1994 to explicitly protect such communications.\(^{13}\) In 2001, the U.S. Supreme Court confirmed that the Wiretap Act “now applies to the interception of conversations over both cellular and cordless phones.”\(^{14}\)

B. Use and Disclosure.

The Wiretap Act is also violated when any person “uses” or “discloses” the contents of an intercepted communication:

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;\(^{15}\)

The Wiretap Act prohibits the disclosure of "any information concerning the substance, purport, or meaning of that communication."\(^{16}\) Therefore, even revealing the general nature of a communication or intimating its contents may constitute an actionable disclosure.\(^{17}\) However, knowledge or reason to know of the illegality is an element of this offense.\(^{18}\)

NOTE: An attorney can have personal criminal and civil liability for using or disclosing an improper recording made by a client. For example, the following can be separate and independent wiretap violations: (1) client disclosure to attorney, (2) attorney’s use of information in pleadings, and (3) attorney’s and client’s disclosures in summary judgment pleadings and affidavits.\(^{19}\) There is no attorney immunity.\(^{20}\)

C. Definitions.

Under the Wiretap Act, statutory definitions are critical.

\(^{11}\) 18 U.S.C. § 2511(1)(a).

\(^{12}\) See e.g., Tyler v. Berodt, 877 F.2d 705 (8th Cir.1989); Askin v. McNulty, 47 F.3d 100 (4th Cir.1995); United States v. Smith, 978 F.2d 171 (5th Cir.1992).


\(^{15}\) 18 U.S.C. § 2511(1)(c), (d).

\(^{16}\) 18 U.S.C. § 2510(8).


\(^{19}\) See, e.g., Nix v. O'Malley, 160 F.3d 343 (6th Cir.1998).

\(^{20}\) Id.
1. **Wire Communication.**

“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.”21 A “wire” communication must be “aural,” or spoken by a human.22 It must also be transmitted at least in part by a wire. Wire communications are protected against interception regardless of the speaker’s expectation of privacy.23

2. **Oral Communication.**

“Oral communication” means “any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.”24 Typically, oral communications include face-to-face communications where the participants have a reasonable expectation of noninterception. The statute requires a court to determine whether a person had a subjective expectation that her conversations were free from interception, and whether that expectation was objectively reasonable.25 It is not a violation to record oral communications where there is no reasonable expectation of privacy.

3. **Electronic Communication.**

“Electronic communication” means “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system…but does not include any wire or oral communication.”26

D. **Penalties.**

1. **Criminal.**

Criminal penalties for a violation of the Wiretap Act include a fine, imprisonment up to five years, or both.26

2. **Civil.**

The Wiretap Act also provides a civil cause of action for “any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used.”27 The Wiretap Act provides for civil remedies including equitable relief (injunctions), damages, punitive damages, and reasonable attorney’s fees and costs.28 As damages, the court may assess the greater of:

   a. Actual damages,
   b. Statutory damages of $100 a day for each day of violation, or
   c. $10,000.29

The $10,000 in statutory damages is not per violation, but is a single sum that applies to a closely-related course of conduct over a relatively short period of time.30 However, if multiple persons’ communications were intercepted, the statutory damages are per plaintiff.31 There is a split among federal circuits as to whether the $10,000 amount is a minimum that must be awarded or whether a court has the discretion to decline to award that amount.

Courts holding that damages are discretionary:

- *Reynolds v. Spears*, 93 F.3d 428 (8th Cir. 1996)

Courts holding that damages are mandatory:

- *Rodgers v. Wood*, 910 F.2d 444 (7th Cir. 1990)

In order to obtain punitive damages, a party must prove a wanton, reckless, or malicious violation.32 Courts have ruled that if a party had some sort of legitimate explanation for the recordings, then punitive damages are not merited.33

Wiretap Act claims are likely to become more frequent when attorneys realize that the law provides for large statutory damages in addition to attorney’s fees.

**Federal Example – Rodgers v. Wood**

*Rodgers v. Wood*, 910 F.2d 444 (7th Cir.1990). Milwaukee police officers were executing a search warrant and used a phone in the home to trace serial numbers on merchandise and also to call a TV show

---

29 18 U.S.C. § 2520(c).
31 *Id.*
33 *Id.*
The homeowner had a recording device installed, which recorded all calls. The recording of the conversation with the TV host showed that the officers had previously contacted the host and revealed the fact that they would be searching the residence for stolen goods. In Wisconsin, it was against the law to disclose the issuance of a search warrant prior to its execution. The homeowner gave the recordings to his attorney. During the attorney’s representation, the attorney disclosed the contents of the police officers’ taped telephone conversations on at least four occasions, including to the district attorney, the Internal Affairs Division, and in a document filed in connection with sentencing in the underlying case. The police officers sued the attorney in federal court, under the civil cause of action contained in the Wiretap Act. The attorney stipulated that the wire communication was unauthorized under the Act and that it was disclosed without permission. However, he argued that his disclosures were protected by common law privileges attaching to persons reporting criminal activity and by an attorney-client privilege. The court rejected the defenses, granted the officers’ motion for summary judgment, and imposed statutory damages of $20,000 against the attorney.

Federal Example – Bess v. Bess

_Bess v. Bess_, 929 F.2d 1332, 1335 (8th Cir. 1991). Husband and wife separated after 26 years of marriage. Several months prior to separation, Husband attached a hidden tape recorder to the basement telephone line of the marital residence, which operated intermittently until Wife found and removed it. After the divorce was final, ex-Wife filed suit against ex-Husband for wiretap violations. At trial ex-Wife introduced 12 tapes containing her intercepted phone conversations, with an average of 2.5 conversations each, and representing one day of interception per tape. Ex-Wife further introduced transcripts from the divorce trial in which ex-Husband used information derived from the intercepted conversations. The trial judge granted the Wiretap claim, found 12 days of interception, and awarded statutory damages of $1,200 ($100 for each day of violation) plus attorney’s fees. The appellate court added one additional day of violation for the use and disclosure at the divorce trial.

Federal Example – Leach v. Byram

_Leach v. Byram_, 68 F.Supp.2d 1072, 1075 (D.Minn. 1999). There was a civil case between family members regarding the dissolution of a business partnership. The father had recorded the son’s phone calls by using a police scanner tuned to the frequency of his portable phone. The father’s attorney sent a letter to the son’s attorney stating that he had reviewed the tapes, would provide copies, and that the tapes contained significant admissions and impeachment material regarding misuse of partnership funds, insurance fraud, and other illegal activity. The attorney stated “it will be interesting to see how your client’s and witness’ credibility stand up after discussing some of these past statements.” The letter then went on to discuss settlement options. The parties settled the case, and the son and his wife agreed not to pursue interception claims against the father. The son and his wife then sued the father’s attorney for a Wiretap Act violation. The court held that the attorney intentionally used the contents of an intercepted communication provided to him by his client, in violation of the Wiretap Act. The court found that the letter from the father’s attorney to the son’s attorney contained a veiled threat to use the information for impeachment at trial and that sufficed as a "use" under the statute. The attorney argued that the use was not intentional and that he did not know that the information came from a prohibited interception. The court found that the evidence showed that the attorney knew of the interceptions before sending the letter, and that he deliberately used that knowledge to procure a settlement. The court found that it had discretion in the amount of statutory damages and that it would be unjust to require the attorney to pay damages. However, the attorney was ordered to pay attorney’s fees.


Wiretap Act claims are subject to a two-year statute of limitations. The statute of limitations begins to run when the claimant first has a reasonable opportunity to discover the violation. It does not require the claimant to have actual knowledge of the violation; only that the claimant have a reasonable opportunity to discover it. However, even if the statute of limitations has run for the original interception, each “use” or “disclosure” is a separate offense and is subject to a separate two-year limitations period.

E. Exclusionary Rule.

The Wiretap Act contains a strict exclusionary rule, prohibiting intercepted communications from being used in any proceeding:

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other

34 18 U.S.C. § 2520(e).
35 Id.
36 Davis v. Zirkelbach, 149 F.3d 614, 618 (7th Cir.1998).
proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.\(^{38}\)

Criminal lawyers are familiar with exclusionary rules. However, Texas law only prohibits the introduction of illegally-obtained evidence in criminal trials.\(^{39}\) Generally, illegally-obtained evidence is admissible in civil trials.\(^{40}\) The Wiretap Act overrides this practice and specifically provides that evidence obtained in violation of the Act may not be used in any proceeding—civil, criminal, administrative, or otherwise. By excluding “evidence derived therefrom,” the Wiretap Act also excludes “fruits of the poisonous tree”—any evidence obtained as a result of the intercepted communication.\(^{41}\) Unlike the Fourth Amendment, the Wiretap Act applies to private conduct as well as to governmental agents.\(^{42}\)

**NOTE:** the exclusionary rule applies to “wire” or “oral” communications—not “electronic” communications. For example, this means that intercepted text messages would not be covered by the exclusionary rule. This example underscores the importance of a close reading of the statute and all defined terms.

Currently, as long as the communication is a voice communication, it will be subject to the stronger protections accorded to “wire” communications. That means that the exclusionary rule would apply to landline calls, cellular calls, and VoIP or internet calls (Skype, etc.).\(^{43}\)

F. **Consent.**

1. **One-Party Consent.**

   The Wiretap Act contains an explicit exception for communications “intercepted” by one of the parties to the communication. The Act provides:

   (d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception....\(^{44}\)

   In other words, any person may record any conversation to which he or she is a party. This is known as “one-party consent.” Federal law and the laws of 38 states (including Texas) provide that only one person’s consent to a recording is needed. Additionally, any further use or disclosure of such a recording is permissible and is not a violation of the Wiretap Act.

2. **All-Party Consent.**

   Twelve states, however, require that all parties must consent to a recording. Those states include California, Connecticut, Florida, Hawaii (under some circumstances), Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania, and Washington. In an all-party consent state, there may be criminal and civil penalties for recording or intercepting a communication without the consent of every party. Further, any subsequent use or disclosure of communications recorded without the consent of all parties may be additional violations under the law of those states (but not under federal law). If a call is conducted across state lines, the law of the stricter state applies. Therefore, it is best to advise clients not to record conversations if any party is outside Texas.

3. **No Spousal Exception.**

   Early in the history of the Wiretap Act, some courts held that there was an implied exception for spouses, meaning there was no violation for one spouse intercepting communications of the other spouse.\(^{45}\) Those opinions were widely criticized.\(^{46}\) A Texas case explicitly held that there is no exemption for spouses under the Wiretap Act, and that a spouse can be in violation for intercepting the other spouse’s communications.

---

41 United States v. Smith, 155 F.3d 1051, 1059 (9th Cir.1998).
42 United States v. Steiger, 318 F.3d 1039, 1046 (11th Cir. 2003).
Texas Example – Collins v. Collins

_Collins v. Collins_, 904 S.W.2d 792 (Tex.App.-Houston [1st Dist.] 1995, writ denied). The following is from the holding of the Collins court. Two Texas courts of appeals have held that held that the interception of a telephone conversation by a spouse is illegal. Neither the state nor the federal wiretap statutes contain any exception for wiretaps between spouses. Texas courts have long recognized both a common law and a constitutional right of privacy. Nothing in the Texas Constitution or our common law suggests that the right of privacy is limited to unmarried individuals. Further, the legislative history of the federal wiretap statute indicates that Congress anticipated it would restrict the use of wiretap evidence in divorce cases. Two senators specifically stated that the "three major areas in which private electronic surveillance was widespread were (1) industrial, (2) divorce cases, and (3) politics;" and "[a] broad prohibition is imposed on private use of electronic surveillance, particularly in domestic relations and industrial espionage situations."

4. Vicarious Consent

A common fact pattern involves one parent who intercepts communications between the child and the other parent. Because parents generally have the ability to provide legal consent on behalf of minor children, there is lots of case law interpreting the circumstances under which one parent can consent to recording communications between the child and others.

Some federal courts have found that where the parent has a good faith, objectively reasonable belief that the recording is necessary for the welfare of the child, a vicarious consent exception to the Wiretap Act will make such recordings permissible. Texas state courts have followed this interpretation.

Texas Example – Alameda v. State

_Alameda v. State_, 235 S.W.3d 218, 223 (Tex.Crim.App.2007). While the defendant was going through a divorce, he moved in with a woman and her 12-year-old daughter. After he moved out, the mother became suspicious that he and her daughter were communicating. She installed a recording device on the home phone. Over a two-week period, she recorded almost 20 hours of calls between the then 13-year-old daughter and the defendant, showing that they were having a sexual relationship. The mother took the tapes to the police, and the defendant was charged. The defendant moved to suppress the tapes, claiming they were recorded in violation of Tex. Penal Code § 16.02 [Texas wiretap law] and were therefore inadmissible under Code Crim. Proc. art. 38.23 [Texas exclusionary rule]. The trial judge held that the mother could vicariously consent to recordings of her daughter’s conversations. The Texas Court of Criminal Appeals held that it was not error for the trial court to admit the tapes and that vicarious-consent is acceptable if a parent has an objectively reasonable, good-faith belief that consenting for the child was in the child's best interest. The court stated that this did not amount to adding a new exception to the wiretap statute. The court held that vicarious-consent, which is a type of consent recognized in many contexts in the law regarding the parent-child relationship, also applies to the existing consent exception to the wiretap statute.

Texas Example – Allen v. Mancini

_Allen v. Mancini_, 170 S.W.3d 167 (Tex.App.-Eastland 2005, pet. denied). In a custody modification case, a father recorded conversations between his child and the mother. The mother appealed the admission of the recordings at trial under the Wiretap Act. The appellate court held that since the father was a managing conservator with authority to consent to various decisions regarding the child, he had the authority to consent on behalf of the child to the tape recording of conversations between the child and the mother. The appellate court stated that a parent may vicariously consent to the tape-recording of a minor child as long as the parent has a good faith, objectively reasonable basis for believing that it is necessary and in the best interest of the child to consent on behalf of his or her minor child to the tape recording.

V. TEXAS STATE WIRETAPPING LAW.

Texas has its own state wiretapping law, contained in the Penal Code. The Texas law is designed to closely parallel the federal law, although it differs in some respects.

A. Offense.

Under the Texas wiretapping law, it is an offense if a person:

1. intentionally _intercepts_, endeavors to intercept, or procures another person to intercept or endeavor to intercept a wire, oral, or electronic communication;
2. intentionally _discloses_ or endeavors to disclose to another person the contents of a

---

50 Tex. Penal Code § 16.02.
wire, oral, or electronic communication if the person knows or has reason to know the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(3) intentionally uses or endeavors to use the contents of a wire, oral, or electronic communication if the person knows or is reckless about whether the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(4) knowingly or intentionally effects a covert entry for the purpose of intercepting wire, oral, or electronic communications without court order or authorization; or

(5) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication....

The offenses and definitions generally parallel the federal Act, although Texas added an offense for effecting a covert entry for the purpose of intercepting communications. The defined terms, including “wire,” “oral,” and “electronic” communications, also parallel the federal Act. The Texas law also specifically enumerates a variety of affirmative defenses, including the one-party consent requirement.

One key difference is the knowledge requirement for a “use” offense. Under the federal Wiretap Act, a person commits an offense if the person uses the contents of an intercepted communication “knowing or having reason to know” that the information was obtained through interception. Under the Texas law, a person commits an offense if the person uses the contents of an intercepted communication if the person “knows or is reckless about” whether the information was obtained through interception. This is a broader definition and includes more conduct than the federal Act.

B. Penalties.

1. Criminal.
   A violation of the Texas wiretap law is a 2nd degree felony.

2. Civil.
   The Texas Civil Practice and Remedies Code contains a civil cause of action for interception of communication:

   A party to a communication may sue a person who:

   (1) intercepts, attempts to intercept, or employs or obtains another to intercept or attempt to intercept the communication;
   (2) uses or divulges information that he knows or reasonably should know was obtained by interception of the communication...

   For the purpose of the civil claim, a communication is defined as “speech uttered by a person” or “information including speech that is transmitted in whole or in part with the aid of a wire or cable.” This definition likely parallels “oral” communications and “wire” communications under the state and federal wiretap laws, so case law interpreting those terms would provide some guidance. Like the federal Wiretap Act, a person must be a party to the communication to have standing to sue under this law.

   3. Damages.
      Under the federal Wiretap Act, most courts have interpreted the statutory damages provision to be discretionary, because the statute uses the term “may.” The Texas cause of action differs, and provides that a person is entitled to:

      (1) an injunction prohibiting a further interception, attempted interception, or divulgence or use of information obtained by an interception;
      (2) statutory damages of $10,000 for each occurrence;
      (3) all actual damages in excess of $10,000;
      (4) punitive damages in an amount determined by the court or jury; and
      (5) reasonable attorney's fees and costs.

   While courts have held that the federal Wiretap Act provides total statutory damages of $10,000, the Texas civil claim allows statutory damages for “each occurrence.” It is yet to be determined whether Texas courts will define “occurrence” to mean each interception or follow the federal meaning of a “closely-related course of conduct over a relatively short period of time.” Additionally, one court has held that the punitive damages are not subject to any statutory cap. However, the relevant statute has been amended since that decision.

---

51 Tex. Penal Code § 16.02(b) (emph. added).
52 Tex. Penal Code § 16.02(c).
53 Tex. Penal Code § 16.02(f).
56 Dorris v. Absher, 179 F.3d 420, 428 (6th Cir.1999).
57 Parker v. Parker, 897 S.W.2d 918, 930 (Tex. App.—Fort Worth 1995, writ denied).
VI. OVERLAP BETWEEN WIRETAP ACT AND STORED COMMUNICATIONS ACT.

The Stored Communications Act is discussed below, but the two laws overlap in confusing ways. 58 Although the Wiretap Act is generally thought to apply to voice communications, it can also apply to interception of data. However, the Wiretap Act applies only to data intercepted contemporaneously with transmission. 59 Stored e-mail cannot be intercepted under the Wiretap Act. 60 Very few seizures of electronic communications from computers will constitute interceptions under the Wiretap Act:

[T]here is only a narrow window during which an E-mail interception may occur — the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible. 61

However, there are spyware programs that automatically forward electronic communications contemporaneous with transmission, and the use of such programs may constitute a violation of the Wiretap Act. The Stored Communications Act applies to data in electronic storage and thus provides broader protection against data interception. However, the Stored Communications Act does not contain an exclusionary rule or create a suppression remedy. 62 It may benefit a client to argue that a particular interception is a breach of the Wiretap Act:

[i]the level of protection provided stored communications under the SCA is considerably less than that provided by communications covered by the Wiretap Act.... [If] acquisition of a stored communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the SCA. Congress could not have intended this result. 63

VII. FEDERAL STORED COMMUNICATIONS ACT.

The Stored Communications Act has been amended several times, with the last substantive changes occurring in 2002. While it overlaps the Wiretap Act, it differs from it in key respects.

A. Offense

The Stored Communications Act makes it an offense to:

1. intentionally accesses without authorization a facility through which an electronic communication service is provided; or
2. intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.... 64

While the Wiretap Act focuses on interceptions that happen contemporaneously with transmission, the Stored Communications Act focuses on accessing communications in electronic storage, as that term is statutorily defined.

B. Definitions

1. Wire and Electronic Communications.

The Stored Communications Act adopts by reference the statutory definitions of the Wiretap Act. The Stored Communications Act refers solely to “wire” and “electronic” communications, omitting the “oral” communication coverage of the Wiretap Act.

2. Electronic Storage.

A threshold issue for the Stored Communications Act is whether a communication is in “electronic storage.” The term is statutorily defined to mean:

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

68 United States v. Smith, 155 F.3d 1051, 1055 (9th Cir.1998) (the intersection of these two statutes "is a complex, often convoluted, area of the law").
61 United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir.2003).
62 United States v. Steiger, 318 F.3d 1039, 1051 (11th Cir.2003).
63 Konop, 302 F.3d at 879; see also Steve Jackson Games, 36 F.3d at 463.
64 18 U.S.C. § 2701(a).
(B) any storage of such communication by an
electronic communication service for
purposes of backup protection of such
communication;

Courts have struggled to define “temporary,
intermediate storage” in the context of how data is
stored and transmitted over the internet. For example,
it is not a violation to obtain answering machine
messages located on a physical recorder, but it is a
violation to access voicemail messages stored on a
telecommunications system.65 Similarly, the Stored
Communications Act is not violated when someone
accesses emails that are stored locally on a computer, but
it can be a violation to access webmail that is stored on
the internet.66 There is some disagreement about
whether e-mail that is intercepted after it has been
received and read is in “temporary, intermediate
storage,” “backup storage,” or “post-transmission
storage.” The first two categories would be protected
under the Stored Communications Act, while the third
would not.

Federal Example – Fraser v. Nationwide

Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107,
114 (3d Cir.2003). Nationwide, Fraser’s employer,
thought he was communicating with competitors, so
the company searched his e-mail that was stored on its
main file server. Fraser alleged violations of the
Wiretap Act, the Stored Communications Act, and
state law. The District Court granted summary
judgment in favor of Nationwide on the Stored
Communications Act claim, holding that the law did
not apply to the e-mails at issue because the
transmissions were neither in "temporary, intermediate
storage" nor in "backup" storage. Rather, according to
the District Court, the e-mail was in a state it described
as "post-transmission storage." The appellate court
agreed that Fraser’s e-mail was not in temporary,
intermediate storage. But the court stated that it seems
questionable that the transmissions were not in backup
storage — a term that neither the statute nor the
legislative history defines. The appellate court affirmed
through a different analytical path, assuming without
deciding that the e-mails were in backup storage. The
court applied an exception in the law for
communications service providers, and held that since
the e-mail was stored on Nationwide’s system, which
Nationwide administered, that the e-mails were not
protected.

Federal Example – U.S. v. Steiger

An anonymous source installed a Trojan horse
virus on Steiger’s computer, accessed his files, and
found child pornography, which the hacker reported by
e-mail to the police in Montgomery, Alabama. The
hacker was a self-appointed vigilante in Turkey whose
hobby was to post the disguised virus on child
pornography news groups, access the computers of
users who downloaded it, and then report them. On
appeal, the court held that the Wiretap Act did not
exclude the evidence because it was not intercepted
contemporaneously with transmission. The court also
held that the Stored Communications Act did not apply
because the hacker accessed Steiger’s computer
directly, and did not access the files while they were in
storage with an electronic communication service. The
court held that the Stored Communications Act does
not apply to hacking into personal computers to
retrieve information stored therein.

C. Penalties.

1. Criminal.

Criminal penalties vary with the purpose of the
offense and whether or not it is a first offense:67

<table>
<thead>
<tr>
<th>Purpose</th>
<th>First Offense</th>
<th>Subsequent Offense</th>
</tr>
</thead>
<tbody>
<tr>
<td>commercial advantage, malicious</td>
<td>Fine or imprisonment for not</td>
<td>fine or imprisonment for not more</td>
</tr>
<tr>
<td>destruction or damage, or private</td>
<td>more than 5 years, or both</td>
<td>more than 10 years, or both</td>
</tr>
<tr>
<td>commercial gain, or in furtherance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>of any criminal or tortious act</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other purpose</td>
<td>fine or imprisonment for not</td>
<td>fine or imprisonment for not more</td>
</tr>
<tr>
<td></td>
<td>more than 1 year or both</td>
<td>more than 5 years, or both</td>
</tr>
</tbody>
</table>

2. Civil.

The Stored Communications Act permits a
broader group of people to bring civil claims,
compared to the Wiretap Act. While the Wiretap Act
only permits a person whose communication was
intercepted to sue, the Stored Communications Act
permits:

…[any] person aggrieved by any violation of
this chapter in which the conduct constituting
the violation is engaged in with a knowing or

65 See, e.g., U.S. v. Smith, 155 F.3d 1051, 1056 (9th Cir.
1998).
66 See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868,
874-880 (9th Cir. 2002).
intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.\(^{68}\)

Relief available in a civil claim under the Stored Communications Act includes:\(^{69}\)

- preliminary, equitable, or declaratory relief, including injunctions;
- actual damages including any profits made by the violator as a result of the violation;
- minimum statutory damages of $1,000;
- punitive damages if the violation is willful or intentional; and
- reasonable attorney’s fees and litigation costs.

Like the Wiretap Act, the Stored Communications Act is subject to a two-year statute of limitations.\(^{70}\) The statute of limitations begins to run when a claimant has “inquiry notice” that her rights might have been invaded.\(^{71}\)

VIII. TEXAS STATE STORED COMMUNICATIONS LAW.
Texas has its own law regarding unlawful access to stored communications. Under the Texas law, it is an offense if a person:

...obtains, alters, or prevents authorized access to a wire or electronic communication while the communication is in electronic storage by:

(1) intentionally obtaining access without authorization to a facility through which a wire or electronic communications service is provided; or

(2) intentionally exceeding an authorization for access to a facility through which a wire or electronic communications service is provided.\(^{72}\)

The Texas law is virtually identical to the federal law. If the offense is committed to obtain a benefit or to harm another, it is a state jail felony; otherwise, it is a class A misdemeanor.\(^{73}\)

---

\(^{68}\) 18 U.S.C. § 2707(a).
\(^{69}\) 18 U.S.C. 2710(b), (c).
\(^{70}\) 18 U.S.C. § 2707(f).
\(^{71}\) Davis v. Zirkelbach, 149 F.3d 614, 618 (7th Cir.1998).
\(^{72}\) Tex. Penal Code § 16.04(b).
\(^{73}\) Tex. Penal Code § 16.04(c), (d).
officers violated her First Amendment right by filing the wiretapping charge without probable cause in retaliation for her attempted filming. The court held that First Amendment principles apply to the filming of a traffic stop—the subject of filming is "police carrying out their duties in public." A traffic stop, no matter the additional circumstances, is inescapably a police duty carried out in public. Hence, a traffic stop does not extinguish an individual's right to film. This is not to say, however, that an individual's exercise of the right to film a traffic stop cannot be limited. Reasonable restrictions on the exercise of the right to film may be imposed when the circumstances justify them. The circumstances of some traffic stops, particularly when the detained individual is armed, might justify a safety measure—for example, a command that bystanders disperse—that would incidentally impact an individual's exercise of the First Amendment right to film. Such an order, even when directed at a person who is filming, may be appropriate for legitimate safety reasons. However, a police order that is specifically directed at the First Amendment right to film police performing their duties in public may be constitutionally imposed only if the officer can reasonably conclude that the filming itself is interfering, or is about to interfere, with his duties. Importantly, an individual's exercise of her First Amendment right to film police activity carried out in public, including a traffic stop, necessarily remains unfettered unless and until a reasonable restriction is imposed or in place.

B. Recording Public Figures

In the Bartnicki case,74 the United States Supreme Court found a First Amendment exception to the wiretap laws where a person publishes communications relevant to matter of public concern that were illegally intercepted by a third party. During collective bargaining negotiations between a teachers’ union and a school board, the union’s chief negotiator held a cell phone call with the union president to discuss details of the negotiations. An unidentified person intercepted and recorded the call and sent the recording to the head of a local taxpayers’ organization. That person distributed the tape to radio, television, and newspaper media, who broadcast the contents. The two persons involved in the original call sued everyone for using and disclosing wiretapped communications. The defendants claimed their publication of truthful information of public importance was protected by the First Amendment. The Supreme Court refused to address the broader questions of whether truthful publication may ever be punished consistent with the First Amendment, or whether the government may punish the publication of information that was acquired unlawfully by media. Limiting the question to the case, where the media lawfully acquired an intercepted conversation, the Court permitted a First Amendment exception. The Court held that the underlying interest of the wiretap law was to protect privacy and deter invasions of privacy. However, punishing people for publishing the information would not effectively deter an anonymous wiretapper. The Court held that “a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern.”

C. Online Threats

The United States Supreme Court has just agreed to hear an appeal of a man sentenced to four years in federal prison for posting violent online rants against his estranged wife, law enforcement officials, and former co-workers.75 The man claimed that he was writing rap lyrics as a way of venting his emotions, and that his statements were protected by the First Amendment. The issue is which standard should apply: (1) an objective standard of whether a reasonable person would consider the statements threatening or (2) a subjective standard of whether the person making the statements intended them to be understood as threats. The side arguing for a subjective intent standard points out that a person cannot control how his content is reposted and distributed over the internet or what the audience for the statements will end up being. However, the other side focuses on the extreme and shocking content and the real effects on the target of the communications. The Supreme Court granted the petition for review on June 16, 2014, and requested briefing, so the outcome will not be known for several months.

X. OTHER TEXAS COMPUTER CRIMES.

A. Online Impersonation.

Texas was one of the first states to implement a law prohibiting online impersonation when it passed Tex. Penal Code § 33.07 in 2009. The law creates two offenses:

(a) A person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to:

(1) create a web page on a commercial social networking site or other Internet website; or


(2) post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail program or message board program.

(b) A person commits an offense if the person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:

1. without obtaining the other person’s consent;
2. with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and
3. with the intent to harm or defraud any person.

An offense under subsection (a) is a third-degree felony. An offense under subsection (b) is a Class A misdemeanor, unless the actor commits the offense with the intent to solicit a response by emergency personnel, in which case it is a third-degree felony. If the same conduct constitutes a violation of multiple sections of the Penal Code, the person may be prosecuted under any or all of the laws. The law carves out a defense for employees of social networking sites, internet service providers, etc.

Under this law, the defendant must have the intent to harm the victim. The penal code defines "harm" as "anything reasonably regarded as loss, disadvantage, or injury." There is no requirement that the harm be physical harm. Emotional distress can be sufficient to qualify as harm under the Penal Code.

Another crucial element of this offense is the impersonation. If a person merely uses the internet to harm someone, without impersonating, the conduct would not be covered by this section. Rather, it would likely be considered harassment under Tex. Penal Code § 42.07. It is interesting to note that harassment is a misdemeanor, while impersonation is a felony.

Texas Example – Taylor v. State
Taylor v. State, No. 02-11-00092-CR (Tex.App.—Fort Worth Mar. 22, 2012) (memo. op.). A woman provided psychic services through her website. She began to receive rude and obscene online chat messages from someone. She received a package in the mail containing what appeared to be a used condom (later found to contain soy milk). She then began to receive messages purportedly from her hairdresser. The “hairdresser” set up a meeting, and when no one showed up, the psychic contacted the hairdresser and found out the communications were not from her. The imposter hairdresser continued to send her messages. The psychic then received a second package containing what appeared to be soiled panties. The police tracked down the man responsible, and he admitted to everything. He was charged with online harassment under Tex. Penal Code § 33.07. That law requires, however, that a person have the intent to harm. The defendant claimed that his intent was not to harm, but rather to test the victim’s psychic abilities. The court upheld the conviction, finding that the evidence could have shown an intent to harm.


The Penal Code contains a criminal offense for breach of computer security. The first level of offense does not require that the defendant have any intent to harm:

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

The knowledge requirement applies to both the access and consent elements of the offense. An offense under subsection (a) is a Class B misdemeanor, except that the offense is a state jail felony if the defendant has been previously convicted two or more times or if the system is owned by the government or a critical infrastructure facility.

The second level of offense has more severe penalties, but requires that the defendant have intent to harm:

(b-1) A person commits an offense if with the intent to defraud or harm another or

---

76 Tex. Penal Code § 33.07(c).
77 Id.
78 Tex. Penal Code § 33.07(d).
79 Tex. Penal Code § 33.07(e).
83 Tex. Penal Code § 33.02(a).
85 Tex. Penal Code § 33.02(b).
alter, damage, or delete property, the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

The penalty for an offense under this subsection varies with the “amount involved.”

<table>
<thead>
<tr>
<th>Penalty</th>
<th>Aggregate Amount Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>State jail felony</td>
<td>&lt; $20,000</td>
</tr>
<tr>
<td>3rd degree felony</td>
<td>≥ $20,000, &lt; $100,000</td>
</tr>
<tr>
<td>2nd degree felony</td>
<td>≥ $100,000, &lt; $200,000</td>
</tr>
<tr>
<td>1st degree felony</td>
<td>&gt; $200,000</td>
</tr>
</tbody>
</table>

It is a second degree felony to obtain the identifying information of another by accessing only one computer, computer network, or computer system; or a third degree felony if more than one.

A person acts without effective consent if the consent was "used for a purpose other than that for which the consent was given." Under the statute, "access" means "to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system." A jury may infer knowledge or intent from the acts, conduct, and remarks of the accused, and from the surrounding circumstances. Direct evidence of the elements of the offense is not required. Proof of a culpable mental state almost invariably depends upon circumstantial evidence. Juries are permitted to make multiple reasonable inferences from the evidence presented at trial, and circumstantial evidence is as probative as direct evidence in establishing the guilt of an actor. Circumstantial evidence alone can be sufficient to establish guilt.

Federal Example – U.S. v. Stanley

United States v. Stanley, No. 13-1910 (3d Cir. 2014), released June 11, 2014, involved whether a person has a reasonable expectation of privacy when he connects to another person’s unsecured wi-fi internet connection (he doesn’t). Importantly, the opinion contains dicta implying that accessing an unsecured, open wi-fi network may be a violation of state law:

A large number of states, including Pennsylvania, have criminalized unauthorized access to a computer network. A number of states have also passed statutes penalizing theft of services, which often explicitly include telephone, cable, or computer services. We need not decide here whether these statutes apply to wireless mooching..

Texas Example – Muhammed v. State

Muhammed v. State, 331 S.W.3d 187 (Tex.App.-Houston [14th Dist.] 2011, pet. ref'd). The victim and the defendant both attended the University of Houston. The victim began receiving emails to one of his UH accounts from an unknown Yahoo account, including one which contained his social security number and others about his personal life. His UH account was hacked, his password changed, and his schoolwork deleted. He received notice from the college that there had been a request to change his major. He began to notice a woman waiting for him outside his classrooms, observing him at the Metro bus stop, and following him around the UH campus. She sent him a "friend request" on Facebook. When other UH students reported similar problems, the police investigated. The police got information from UH’s information technology department which led them to the defendant. An officer observed her in the computer lab, walked behind her, and observed her accessing others’ information on the UH website. The defendant denied everything but was found guilty, sentenced to 180 days confinement, and placed on community supervision for two years.

Texas Example – Brackens v. State

Brackens v. State, 312 S.W.3d 831 (Tex.App.-Houston [1st Dist.] 2009, pet. ref'd). The defendant took his laptop to Circuit City to have his data backed up to an external hard drive. In the course of doing the work, the computer technician found child pornography and notified police. On appeal, the defendant argued that the trial court erred in denying his motion to suppress evidence because, among other things, the technician, by opening his computer file, committed the offense of breach of computer security under § 33.02 and therefore all of the files should be suppressed.

86 Tex. Penal Code § 33.02(b-2).
87 Id.
88 Tex. Penal Code § 33.01(12)(E).
89 Tex. Penal Code § 33.01(1).
93 Hooper, 214 S.W.3d at 14-16.
94 Id. at 15.
excluded from evidence. However, the defendant did not place any limitations on his request to back up his computer files. In order to fulfill the defendant’s request, the technician had to copy the defendant’s files onto a DVD to ultimately load the files into the store computer which had the external hard drive connected to it. Once he saw the suspect "Pedo" file, the technician had to open it to confirm that it was not illegal. The testimony supports an implied finding that the defendant’s computer files were accessed in the course of carrying out his work order. Therefore, the technician did not violate section 33.02.

C. Civil Cause of Action.
Chapter 143 of the Civil Practice and Remedies Code creates a cause of action for a person who is injured or whose property is injured by an intentional or knowing violation of Chapter 33 of the Penal Code. This includes both the online impersonation and breach of computer security offenses described above. The civil cause of action permits a person to recover actual damages and reasonable attorney’s fees and costs.

XI. CONCLUSION
These statutes form a technical and complex web of laws that affect criminal practices in potentially far-reaching ways. This paper is an overview of a field with significant depth, and interested practitioners should devote time to reading the statutes and the cases interpreting and applying them.

Filming the Watchmen: Why the First Amendment Protects Your Right to Film the Police in Public Places
Evan Bernick and Paul J. Larkin, Jr.

Abstract
Police are relying on state wiretapping statutes to arrest citizens who film police in public. The federal circuit courts that recognize a First Amendment right to film police in public places where the citizen-recorder has a right to be present are in line with Supreme Court precedent. While the exercise of the right to film police is subject to reasonable time, place, and manner restrictions, police cannot be allowed to suppress speech at the core of the First Amendment’s protections. State wiretapping statutes that prevent citizens from filming police officers in such places without any further justification violate citizens’ First Amendment rights.

B
randy Berning spent the night in a Florida jail because she used a cell phone to film a traffic stop on I-95.1 George Thompson of Fall River, Massachusetts, claimed that he was verbally abused, arrested, and locked up overnight for filming a profane police officer with a cell phone from his front porch. The officer was across the street in full view and within earshot of anyone who happened to be passing by his home.2 Most recently, Florida police arrested and charged Lazaro Estrada with obstruction of justice for peacefully filming an arrest with his cell phone on a public street.3

Why is this happening? Police are unhappy that people are using their cell phones—which often have video capabilities—to film police conduct. Some state statutes generally prohibit the recording or interception of oral communications unless all parties to the conversation consent.4 To prevent citizens from gathering and disseminating information about police conduct, police are relying on these
statutes to arrest citizens who film police in public, even if those citizens have a right to be present in the locations from which they film.

The question arises: Are such filming and any subsequent publication protected by the First Amendment? If so, what can we do to better secure our rights?

This paper summarizes how federal courts of appeal have treated the filming of police officers in public. It then contends that there exists a First Amendment right not only to film police in such places, subject to reasonable time, place, and manner restrictions, but also to publish the content of those films.

State wiretapping statutes that prevent citizens from filming police officers in public places where those citizens have a right to be present violate citizens’ First Amendment rights. While the exercise of the right to film police is subject to reasonable restrictions as to time, place, and manner, police cannot be allowed to suppress speech that is at the core of the First Amendment’s protections.

Circuit Courts Split over the Right to Film Police in Public

Four federal circuits recognize a First Amendment right to film the police in public. The two earlier cases contain little substantive analysis. In Fordyce v. City of Seattle, the Ninth Circuit Court of Appeals recognized “a First Amendment right to film matters of public interest.” The case concerned the filming, for later broadcast, of a protest on a public street, including police activities. The court, however, did not explain why the First Amendment protects a right to film police activities.

In Smith v. City of Cumming, the Eleventh Circuit took up a civil claim under 42 U.S.C. § 1983 in which a citizen-recorder alleged that the police had prevented him from exercising his First Amendment right to videotape police actions. The court cited Fordyce for the proposition that the First Amendment protects the right to “gather information about what public officials do on public property, and specifically, a right to record matters of public interest.” On this basis, the court held that citizens have a First Amendment right, subject to reasonable time, place, and manner restrictions, “to photograph or videotape police conduct.”

Two other circuits have also recognized the right to film the police in public. In Glik v. Cunniffe, the First Circuit decided the case of a man arrested for openly filming an arrest in Boston Common in violation of a Massachusetts wiretapping law that criminalizes nonconsensual recording. The court held that a right to videotape police was “clearly established.” The court cited Smith with several Supreme Court cases that it found established the right to gather and disseminate information about government: “Gathering information about government officials in a form that can readily be disseminated to others serves a cardinal First Amendment interest in protecting and promoting the free discussion of governmental affairs.”

4. See Cal. Penal Code § 632 (1994) (making it a crime to record “confidential communications” in which one of the parties has an objectively reasonable expectation that no one is listening in or overhearing the conversation without the consent of all parties to the conversation); Fla. Stat. Ann. § 934.03 (2013) (making it a crime to intercept or record a “wire, oral, or electronic communication” unless all parties to the communication consent); 720 Ill. Comp. Stat. 5/14 (2008) (making it a crime to use an “eavesdropping device” to overhear or record a phone call or conversation without the consent of all parties to the conversation).
5. 55 F.3d 436, 439 (9th Cir. 1995).
6. 212 F.3d 1332 (11th Cir. 2000).
7. Id. at 1333.
8. Id.
9. 655 F.3d 78 (1st Cir. 2011).
10. Id. at 85.
11. Id. at 82.
The First Circuit recently reaffirmed its Glik decision in *Gericke v. Begin*, ruling that the First Amendment right to videotape a police officer performing a law enforcement action in public includes not only when the police make an arrest in a public park, as in *Glik*, but also when the police stop a vehicle to question the driver.

The Seventh Circuit, in *American Civil Liberties Union of Illinois v. Alvarez*, reached the same conclusion. In *Alvarez*, the ACLU sued Illinois State’s Attorney Anita Alvarez in her official capacity under Section 1983. The ACLU sought to bar Alvarez from enforcing an eavesdropping prohibition against recording activities that the ACLU planned to carry out in connection with its “police accountability program.” The ACLU intended to promote police accountability by openly audio recording police without their consent when (1) the officers were performing their public duties, (2) the officers were in public places, (3) the officers were speaking at a volume audible to the unassisted human ear, and (4) the manner of recording was otherwise lawful.

The Seventh Circuit granted relief. Rejecting the State’s Attorney’s argument that recording is not speech protected by the First Amendment, the court asserted that “restricting the use of an audio or audiovisual recording device suppresses speech just as effectively as restricting the dissemination of the resulting recording.” The court analogized the facts of the case to those of *Citizens United v. Federal Elections Comm’n*, in which the U.S. Supreme Court held that “campaign-finance regulations implicate core First Amendment interests because raising and spending money facilitates the resulting political speech.” Just as raising and spending money facilitates political speech, the Seventh Circuit reasoned that “audio and audiovisual recording are communication technologies, and as such, they enable speech.” To hold that the First Amendment was not implicated would, in a similar fashion, allow the state to “effectively control or suppress speech by the simple expedient of restricting an early step in the speech process rather than the end result.”

By contrast, the Third Circuit does not recognize a First Amendment right to film the police in public. In *Gilles v. Davis* (2005), the Third Circuit suggested that videotaping or photographing the police in the performance of their duties on public property “may be a protected activity,” citing the Eleventh Circuit’s decision in *Smith*. Subsequently, however, in *Kelly v. Borough of Carlisle*, a case that involved the filming of a traffic stop, the Third Circuit did not hold that filming police is protected speech. While the court allowed that a “general right to record matters of public concern” might exist, it concluded that the cases addressing that issue were “insufficiently analogous” to the facts in question to put officers on notice of any such right. It emphasized that no prior case law concerned the filming of a traffic stop.

---

13. *Id.* slip op. 13–21.
14. 679 F.3d 583 (7th Cir. 2012).
15. *Id.* at 588.
16. *Id.* The Illinois eavesdropping statute made it a felony to audio record “all or any part of any conversation” unless all parties to the conversation give their consent. 720 Ill. Comp. Stat. 5/14–2(a)(1) (2006).
17. 679 F.3d at 588.
18. *Id.* at 596.
21. *Id.*
22. 427 F.3d 197, 212 n.14 (3d Cir. 2005). In *Gilles*, two members of a campus ministry, James Gilles and Timothy Petit, brought claims under § 1983 against state university officials, alleging constitutional violations in connection with their arrest following a confrontation with campus police. When a riot broke out following Gilles’s invectives against sex, booze, and homosexuality (delivered in front of a crowd in an area open to the public), police arrested Gilles, together with Petit, who filmed the events. Petit claimed that his First Amendment rights were violated because his videotaping was a protected activity.
23. 622 F.3d 248, 262 (3d Cir. 2010).
24. *Id.*
and that the Supreme Court treats traffic stops as “inherently dangerous.”

The circuit-level decisions recognizing a First Amendment right to film police in public are in line with the Supreme Court’s free speech jurisprudence. In all of the above cases, citizens lawfully acquired publicly available information. The locations where filming took place—streets and parks—were traditional public fora and open to all. In each case, the people filming the police activity had a right to be where they stood when they recorded police conduct. The Supreme Court has consistently held that the First Amendment protects the right to gather publicly available information and to publish that information in any medium of a person’s choosing.

- In *Cox Broadcasting Corp. v. Cohn*, the Court held that a rape victim could not sue a newspaper for damages for publishing the name of a rape victim because the newspaper learned her name through official court records.

- In *Smith v. Daily Mail Pub. Co.*, the Court held that newspapers could lawfully publish the name of a juvenile arrested for homicide. The newspapers had lawfully obtained the name by interviewing witnesses, the police, and an assistant prosecuting attorney. Although a West Virginia statute made it a crime for a newspaper to publish without prior judicial approval the name of any youth charged as a juvenile offender, the Supreme Court ruled the statute unconstitutional because it punished the publication of “lawfully obtained truthful information,” and the government could not point to a countervailing “state interest of the highest order.”

- Finally, in *Bartnicki v. Vopper*, the Court held that a radio commentator possessed a First Amendment right to play a tape of an unlawfully intercepted conversation because he had not played a role in the unlawful interception and had acquired the tape legally.

The right to publish lawfully obtained information does not depend upon the medium of expression. *Cox* and *Smith* both involved newspapers—a medium with which the Framers were familiar and that they would have expected to be the platform for discourse—but the First Amendment protects far more than black-and-white words on newsprint.

In *Burstyn v. Wilson*, the Court held that audio and audiovisual recordings are media of expression that are commonly used for the preservation and dissemination of information and ideas and thus are “included within the free speech and free press guaranty of the First and Fourteenth Amendments.”

The right of publication extends also to the Internet. The Court in *Reno v. American Civil Liberties Union* struck down a congressional statute regulating the transmission of obscene or indecent materials on the Internet, finding no precedent for “qualifying the level of First Amendment scrutiny that should be applied to this medium.”

25. *Id.*
26. See *Hague v. CIO*, 307 U. S. 496, 515 (1939) (streets and parks “have immemorially been held in trust for the use of the public and, time out of mind, have been used for purposes of assembly, communicating thoughts between citizens, and discussing public questions”). The government must carry a heavy burden in order to restrict speech in traditional public fora. See *United States v. Kokinda*, 497 U.S. 720, 726–27 (“Regulation of speech activity on governmental property that has been traditionally open to the public for expressive activity, such as public streets and parks, is examined under strict scrutiny.”).
29. *Id.* at 99.
30. *Id.* at 100.
31. *Id.* at 103.
32. 532 U.S. 514, 530–1 (2001) (“The normal method of deterring unlawful conduct is to impose an appropriate punishment on the person who engages in it…. But it would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party.”).
33. 43 U.S. 495, 502 (1952).
34. 521 U.S. 844, 870 (1997).
Today, citizen-recorders can “stream” police conduct to the Internet as they film that conduct with yet another novel device, smartphones. But while technology has changed, free speech principles remain the same. Filming an event adds only two features to seeing it: The film preserves what the eye saw and corroborates a witness’s account of what he or she viewed. Neither feature should somehow reduce the First Amendment protection that a videographer would be entitled to claim if he or she used binoculars or a camera lens to better observe an event without recording what transpired. The contrary rule would perversely transform a person’s right to observe and report what he or she has seen into the government’s right to demand that someone forget and remain silent about what takes place in a public forum.

The policies that the First Amendment seeks to advance hardly justify any such absurd result. There is a strong public interest in making police officers’ public conduct transparent. Filming the police can yield evidence of government misconduct—among the core concerns of the First Amendment.

Filming and publishing police conduct better informs the public about how officials are conducting their public duties and promotes accountability. Evidence also indicates that it influences law enforcement practice: Police are less likely to engage in misconduct when they know they are being recorded. Finally, police officers have no privacy interests that outweigh the strong public interest in transparency. Police officers conducting their duties in public places cannot reasonably expect that their conduct will be deemed private. Thus, citizen-recorders should be presumptively free to film police in public places where they have the right to be present and to publish their recordings.

The Right to Film the Police in Public

The First Circuit in Glik properly held that the right to film police has limitations. The exercise of First Amendment rights is subject to reasonable time, place, and manner restrictions. In order to protect the First Amendment right to film police officers, it is necessary to define that right and work to ensure that it is respected.

Time, Place, and Manner Restrictions on Filming. The First Amendment does not confer a general right to demand access to a location from which citizens can gather information. In Houchins v. KQED, a media broadcasting company and members of the NAACP sued a sheriff who denied the media access to a portion of a county jail that had been the site of a recent inmate suicide and allegedly abusive conditions. The Court rejected the claim, stating that there is “no basis for the claim that the First Amendment compels others—private persons or governments—to supply information.”

Nor does it give news gatherers free rein to gather news by any means they think necessary. In Branzburg v. Hayes, a case involving journalists who claimed that compelling them to testify about confidential sources would violate their First Amendment right to gather news, the Court held that the First Amendment “does not invalidate every incidental burdening of the press that may result from the enforcement of civil or criminal statutes of general applicability.”

The Court did subsequently recognize a limited right of access in the context of criminal proceedings. In Richmond Newspapers v. Virginia, the Court held that the First Amendment provides the public with a constitutional right of access to criminal trials because they historically had been open to the public and because “it would be difficult to single
out any aspect of government of higher concern and importance to the people.’”

More recently, however, the Court declined to extend the right of access beyond the courtroom. In Los Angeles Police Dept. v. United Reporting Pub. Co., the Court upheld a California law denying access to arrestees’ addresses if the request is made for commercial purposes, stating that the law represented “nothing more than a governmental denial of access to information in its possession.”

Further, the exercise of the right to film police, even where the citizen has a right to be present, cannot be unbounded. The Supreme Court has recognized that the government has a significant interest in protecting safety and has upheld speech restrictions grounded in safety concerns against First Amendment challenges. While cameras are not themselves dangerous, their use can create safety hazards. Citizen-recorders may come too close or approach police from behind or oblique angles, posing a risk to officers looking to minimize their own vulnerabilities as well as those of members of the public. Police must be able to protect their own safety and that of the public.

Yet two caveats are important to remember. First, the police cannot justify the refusal to allow someone to film what is in plain sight on the basis of a time, place, and manner restriction if the purpose of the restriction is to censor what is being seen and recorded. That would be a content-based restriction; Police do not interfere with parents filming their children’s baseball games in public parks. Second, there may be limited circumstances in which the police can justify a content-based restriction. The police can cordon off the area in which offenders have taken a hostage in order to prevent someone from broadcasting police efforts to free the hostage or to preserve the hostage’s privacy. In each case, the government may have a compelling interest in preventing someone from undermining police efforts to free the hostage or in preserving the dignity of a victim who did not volunteer to be on the nightly news.

At the same time, however, the police generally should not be able to blind someone to seeing and reporting what occurs in the open, and they should never be able to do so simply because the film may portray the police in an unfavorable light. The scope of the publication right is one that can and should be filled out using the standard case-by-case approach that the courts have taken in resolving other First Amendment disputes.

**Protecting the Right to Film.** It is critical to prevent the police from invoking the electronic interception laws as a means of choking off constitutionally protected speech when no safety or privacy interests are in play. Certain laws that generally prohibit nonconsensual recording contain exceptions that protect citizens who record what is said in public. For instance, Florida’s wiretapping law provides an exception for in-person communications when the parties do not have a reasonable expectation of


42. 528 U.S. 32, 40 (1999). See also Estes v. Texas, 381 U.S. 532 (1965) (holding that a defendant was deprived of his right under the Fourteenth Amendment to due process by the televising and broadcasting of his trial, even though the court was open to the public and people could observe and report upon the proceedings). Federal courts have long prohibited the broadcasting of their proceedings. See Fed. R. Crim. P. 53 (“Except as otherwise provided by a statute or these rules, the court must not permit the taking of photographs in the courtroom during judicial proceedings or the broadcasting of judicial proceedings from the courtroom.”). The Supreme Court prohibits cameras as well. See, e.g., Public Information Office of the Supreme Court of the United States, A Reporter’s Guide to Applications Pending Before the Supreme Court of the United States 15, at http://www.supremecourt.gov/publicinfo/reportersguide.pdf; Public Information Office of the Supreme Court of the United States, Visitor’s Guide to Oral Argument at the Supreme Court of the United States 3 (reminding visitors that no electronic devices are allowed in the courtroom at any time), at http://www.supremecourt.gov/visiting/visitorsguidetooralargument.pdf.

43. See, e.g., Cox v. New Hampshire, 312 U.S. 569, 574 (1941) (upholding a content-neutral ban on all unlicensed demonstrations “to assure the safety and convenience of the people in the use of public highways”); Madsen v. Women’s Health Ctr., Inc., 512 U.S. 753, 769 (1994) (upholding a content-neutral 36-foot buffer zone to protect access to a clinic and ensure that traffic was not blocked).


45. See Police Dept. of City of Chicago v. Mosley, 408 U.S. 92, 97 (1972) (“Selective exclusions from a public forum may not be based on content alone, and may not be justified by reference to content alone.”).
privacy in the conversation. As noted, the public has a powerful interest in ensuring transparency in law enforcement, and on-duty police officers cannot reasonably expect their public conduct in public places to be private.

Other states, however, do not expressly make such exceptions in their wiretapping statutes. Massachusetts' wiretap statute makes it a crime to "willfully commit[] an interception ... of any wire or oral communication." The statute defines interception to mean "to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication." In Glik, the First Circuit, interpreting that language, concluded that Glik's conduct fell outside the type of clandestine recording targeted by the statute because he openly filmed the officers.

It may be possible to construe those laws as containing an implied exception for instances in which there is no reasonable expectation of privacy. After all, the state legislatures likely did not intend to make it a crime for a local news van to photograph people walking on a municipal sidewalk during the daytime as part of a news story about a beautiful spring afternoon or to photograph spectators at a Yankees game as part of an ESPN roundup. But reading a state law in a manner that excludes such conduct may not always be possible. If that turns out to be true, then the courts will be forced to judge whether the state law violates the First Amendment.

As noted, it would appear that any such law would be unconstitutional. There is no material difference between a case in which someone broadcasts to the officer that he is being filmed and a case in which the filming is entirely secretive. In both cases, the officer has no privacy interest at stake, and the government lacks a compelling interest in preventing citizens from observing the conduct of its agents, either secretly or openly, simply to justify suppressing speech that lies at the core of the First Amendment's protections.

Of course, the government can always charge an erstwhile Steven Spielberg with obstruction of justice or disorderly conduct if he or she physically interferes with police business, but merely filming police business by itself cannot be deemed an obstruction of justice or disorderly conduct. The First Amendment does not allow state law to reach that far.

**Conclusion**

The First Amendment generally protects the right to film police officers in public places and to publish the information acquired. At the same time, the exercise of the right to film, like all First Amendment rights, is subject to limitations. But speech about how public officials are conducting their duties lies at the core of the First Amendment's protections, and filming should therefore be given a wide berth.

Citizen-recorders should be presumptively free to film officers in public places when they have a license to be present, and state laws that authorize officers to prevent them from filming without any further justification are unconstitutional. Even where state wiretapping laws contain exceptions for in-person communications where there is no reasonable expectation of privacy, drafting exceptions that specifically except the filming of police officers in public may help to deter police from suppressing speech. At a minimum, the issue deserves further exploration.

---

46. See Fla. Stat. Ann. § 934.02 (2) (2010) (requiring that an oral communication be "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.").

47. Even in jurisdictions where such exceptions exist, police are using wiretapping laws to suppress speech. One alternative worth exploring is creating specific exceptions for filming on-duty police officers in public. Those exceptions would apply so long as the citizen-recorders violate no other law. The presumption in favor of allowing recording could be overcome in narrow circumstances. Obstruction of justice or disorderly conduct charges could still be brought against citizen-recorders, just as they can be brought against others. Such exemptions for citizen-recorders could help to ensure that they are not treated differently from other citizens. See Cerame, supra note 44, at 449 (arguing that the government should be required to show that "the officer both subjectively believed his or her actions advanced safety, and that a reasonable officer would have objectively believed that those actions advanced safety").


50. Glik, 655 F.3d at 86.