SPOUSAL SPYING

How your online activity is being used against you

ROSEN LAW FIRM
Divorce is Different Here
INTRODUCTION

You suspect your spouse is having an affair. You see the signs, they are vague about their whereabouts, coming home later than usual, being secretive about their text messages. You are hurt, angry, confused, but most of all you want to know the truth.

Thanks to today’s technological advancements, “bugging” a spouse is easier than ever. You can install spyware on a phone or a computer, hide video cameras around the house, and place a GPS tracking device on your spouse’s car. But is any of this legal?

Chances are the “bugging” you are contemplating is illegal – violating both state and federal wiretapping laws and could expose you to serious liability. So think twice before you buy that spyware kit and install it on your spouse’s phone. As much as you want answers about your suspicions, you could find yourself defending a lawsuit in federal court.

This book will guide you through the dos and don’ts of spousal spying by giving you an in depth look at the law, as well as frequently asked questions and examples from recent cases.
I THINK MY SPOUSE IS CHEATING. . .

You have that terrible feeling in your gut, your spouse is being secretive with their cell phone, they are coming home late from work, distancing themselves from you; the signs are all there, you just don't have proof.

Or maybe you’ve recently separated and have reason to believe your spouse was cheating during your marriage.

How can you find out for sure?

Today it seems easier than ever to catch someone cheating. In our technology driven society, recording others has become as easy as tying your shoes. Cell phones come equipped with cameras, video recorders, GPS trackers, and voice recording capability. Tape recorders can easily be purchased at office supply stores at little cost, you can view a step-by-step video showing how to “bug” a room on YouTube, and a simple Google search will provide countless links to purchase spyware.

Despite what popular TV shows and movies may make you think, these sort of recording devices are not simply being used to catch drug dealers and mobsters; increasingly, people are using these devices to catch their spouses cheating.

Why hire a private investigator when you can catch them in the act yourself? The answer is not so simple, and may even carry criminal charges. If you are not careful, using voice recorders, spyware, and other “eavesdropping” devices might give you more legal trouble than relief.
You may be wondering, aside from personal knowledge or peace of mind, why would evidence of an affair be of any importance? Would a judge really care if your spouse cheated on you?

This sort of evidence can in fact have a big impact in certain family law proceedings. For instance, where alimony is concerned, if the “supporting spouse” cheated, the court might be required to automatically award alimony payments to the other spouse. On the other hand, if the “dependent spouse” cheated, it might absolve the supporting spouse from having to pay alimony.

Evidence of marital misconduct is also a factor that the court can consider when making determinations about equitable distribution and custody.

Occasionally, evidence of an affair can impact your case simply by giving you leverage. If your spouse knows you can prove marital misconduct, they may be more agreeable to reaching a settlement without litigation, or they may be more willing to compromise when it comes to splitting certain assets.

Evidence of an affair can also be of value if you plan to take action against the paramour. North Carolina is one of the few remaining states that recognize both alienation of affection and criminal conversation torts, and legally obtained evidence of the affair can substantiate these claims.

**Bottom Line:** Evidence of an affair can impact your case, regardless of whether you plan to litigate your issues or not.
WHY IS RECORDING MY SPOUSE ILLEGAL?

There are both federal and state laws that prohibit recording and spying on your spouse. Without getting too bogged down in the details, here is a brief overview of the laws that prohibit you from “bugging” your spouse.

The Law

I. Federal Law
The Electronic Communications Privacy Act and the Stored Communications Act make it illegal to intercept or gain unauthorized access to certain types of information. There are two subsections we will refer to in this article. The first, referred to as “Title I,” discusses interception of wire, oral, or electronic communication. “Title II” deals with unauthorized access to electronic communications held in electronic storage.

Title I is implicated if you are using a voice activated recording device or certain types of email spyware, and Title II is implicated when you “hack” into your spouse’s email account. All of this is explained in more detail throughout this article, so don’t panic if this seems confusing.

II. State Law
The North Carolina Electronic Surveillance Act provides much of the same information as Title I of the federal law we just mentioned. It prohibits interception of wire, oral, or electronic communications. North Carolina also has laws regarding computer-related crimes that prohibit unlawful access to another person’s computer, system, program, or network without authorization. This most closely mirrors Title II of the federal law.

Additionally, you need to be aware that North Carolina recognizes several privacy tort claims that may also apply. “Intrusion upon seclusion,” which is a fancy way of saying invasion of privacy, is recognized in North Carolina as grounds for a lawsuit. North Carolina also recognizes other torts that could apply depending on the situation, including trespass and intentional or negligent infliction of emotional distress.

Bottom Line: Not only can you be criminally liable for violations under federal and state wiretapping laws for recording conversations or accessing emails of your spouse, you can be sued under several recognized tort claims as well.
Many people consider using tape recorders or voice-activated recorders to catch their spouse. These devises are cheap, easy to use and inconspicuous. So why not hide one in your spouse's car to try to catch them in conversation with their paramour? Because it is illegal.

North Carolina is a “one party consent” state, which means it is illegal to record a conversation without consent (here, “knowledge” = consent) of at least one party. What does that really mean? You may record yourself and your spouse in conversation because you have knowledge and have therefore consented.

No matter how unfair your spouse may find this, as long as you consent to recording the conversation between you two, the recording is not illegal and could be admissible in court. If they admit the affair to you, and you recorded the conversation, it is fair game.

The basic rule to remember is that you cannot record conversations between your spouse and other parties without consent (knowledge) of at least one the parties. Hiding a voice-activated recorder in their car, gym bag, or even in your own home to try to catch him or her with their paramour is illegal. As tempting as it may be to find out the truth about what your spouse is doing in your absence, this is a clear violation of both state and federal wiretapping laws and can be a very costly mistake.

Outside of catching them cheating, there are countless other reasons why using a tape recorder may be helpful to your case. For instance, if your spouse (or ex-spouse) is causing problems during custody exchanges, a tape recording of what took place could help you show your attorney and the judge the type of problems you are experiencing.

If you are a victim of domestic violence, it can be extremely helpful to your case if you have a recording of conversations where your spouse audibly becomes violent. You can probably think of countless other examples where this could apply to your own specific situation. Particularly in family law, it often comes down to he-said/she-said arguments and a recording of a conversation can help shed light on the problems you are experiencing. Just make sure you obtain this recording legally.
Exception to the Rule: Vicarious Consent

There is one exception to the basic rule, which applies if you are recording conversations between your spouse and your children. Several North Carolina cases have said that it is permissible to record your spouse and your children in your absence, so long as you are concerned for the safety of your children.

If you are suspicious of abuse, tape recording conversations between your spouse and your kids might be legal, despite the fact that none of the parties have consented. Keep in mind however, that you may have to defend this fear in court. Simply telling the judge you made the recording because you thought the kids were in danger isn't enough: you will need to backup your suspicion by providing compelling evidence or the judge isn't going to buy it.

Bottom Line: You may use a voice-activated recorder to tape conversations in which you are a party, however it is illegal to tape the conversations of others without consent (knowledge) of at least one party.
CAN I RECORD MY SPOUSE’S PHONE CONVERSATIONS?

Baseline Rule:

Save for a few exceptions, the rules for recording phone conversations are identical to the rules we just touched on that dealt with using voice-activated recorders. As long as one party consents or has knowledge of the recording, it is permissible.

But again, you may not “bug” your home phone or your spouse’s cell phone and record conversations they have with others. It is of no consequence that the home phone belongs to you too, the law is designed to protect the communication; ownership of the phone, or even who pays the phone bill, is irrelevant.

The vicarious consent exception also applies to recording phone conversations, so if you are truly concerned for your children’s safety, you may record conversations between the children and your spouse. Again, be prepared to articulate to a judge why you believed your children’s safety was at issue.

What about recording or accessing voicemails? Courts have held that intercepting a voicemail is also a violation of the federal and state wiretapping laws. Voicemail is considered a wire communication held in electronic storage, which fits squarely within the language of the wiretapping statutes.

Cell Phone Snooping

Today, most of us have cellular or smart phones that house an almost unlimited amount of personal information. Smart phones give their users access to texting, calling, email, calendars, bank account information, and the list goes on.

Say you aren’t interested in actually recording phone calls, but are more concerned with browsing through the contents of their your spouse’s phone. Is this OK?

While there is no case in North Carolina that directly speaks to whether you may scan through your spouse’s cell phone in their absence, most attorneys agree that the permissibility of this would hinge on authorization. Keep in mind that Title II bans unauthorized access to certain information.
We discuss what “authorization” means in depth in the section discussing email access below, but essentially, if your spouse has given you reason to believe that you are allowed to use the phone for various things, you most likely have authorization to take a peek at its contents every now and then.

**Example: Authorized Access v. Unauthorized Access**

When your spouse is aware that you know the passcode to unlock the cell phone, you use the phone from time to time to make calls, check your joint bank account, pull up cartoons on Netflix for your child to watch, pay your cable bill, etc. you have authorization. Generally, your spouse has no expectation of privacy regarding the contents of their cell phone if they know you have the passcode and that you use the phone from time to time.

On the other hand, if you happen to correctly guess the password, or are able to obtain it without their knowledge, you do not have authorization to snoop through the phone.

What if there is no password on the phone? Our advice is that unless your spouse knows you have access to and have in the past used the phone, avoid browsing the phone's contents in your spouse's absence.

**Bottom Line:** You *may* record phone conversations in which you are a party to, however it is illegal to record conversations had by others without consent of at least one party. When it comes to cellular and smart phones, whether you can legally access the contents is largely dependent upon the authorization of the owner.
After reading the previous sections, you may be wondering how “Nanny Cams” can be legal. You know, the stuffed animals with hidden cameras that parents use to monitor babysitters? These do not violate the wiretapping statutes, even if the babysitter has no knowledge of its existence.

Somewhat surprisingly, the rules regarding video recording are in fact different from the rules that apply to voice and telephone recording. Strangely enough, the federal and state wiretapping laws only protect the interception of oral communication like voice-activated recorders and phone tap systems. The statute does not ban video recordings.

This is precisely why “Nanny Cams” have no audio; it is permissible to record video absent an audio feed. As long as you own the property (or otherwise have permission), placing a video recorder may not result in a violation of the federal or state wire tapping laws.

**Bottom Line:** Video recording, with no audio, is permissible if you own the premises or have otherwise obtained permission.
CAN I SNEAK A PEEK INTO MY SPOUSE’S EMAIL ACCOUNT?

So much of our communication takes place over email, so not surprisingly, this is usually what a suspicious spouse will want to tap into first. Most of us have multiple email accounts that are accessible anywhere, including on our cell phones and tablets.

It is also worth mentioning that because it is so easy to delete incoming and outgoing messages, the cheating spouse may actually find it a convenient medium to communicate with the mistress.

People ask us all the time if it’s OK to peek into their spouse’s email, and each time our advice varies depending on the situation. Let’s start with what we know you can’t do.

Spyware: Don’t Do It

It is so tempting; spyware is relatively inexpensive, easy to install, and a surefire way to catch your spouse if they are using email as a means to communicate with a paramour. There are many different types of spyware; some send copies of incoming and outgoing emails to your own email address, others track Internet browsing, and some are even designed to capture and store bank account login information.

People are attracted to spyware because not only can it discover scandalous emails or chats, but also it can provide access to calendars, and even potentially provide details about when and where he or she is spending money. So not only can you discover the illicit emails, but you can also find out when and where he is taking his mistress to dinner? Who wouldn’t want access to that sort of information?

As tempting as it may sound to uncover these details, using these programs is illegal.

Programs like eBlaster that are designed to forward copies of incoming and outgoing messages violate Title I because they intercept these messages contemporaneously with transmission. Use of this type of program violates Title I specifically because interception is simultaneous with transmission. In other words, no time takes place between the generation of the email and your interception of it.

Other types of spyware that are not designed to intercept messages simultaneously with transmission violate Title II rather than Title I, which we discuss below.
CAN I SNEAK A PEEK INTO MY SPOUSE’S EMAIL ACCOUNT?

Accessing Email

Title II covers unauthorized access to electronic communications held in electronic storage. In order to fully understand this, we need to break down each one of the italicized words above.

Authorization: What does this mean? It sounds straightforward enough, but there are several points about authorization worth highlighting. Generally speaking, unauthorized access occurs when you either use a computer or a password without permission. Examples of unauthorized access are as follows:

Looking through a work computer: This applies to computers at an office, or laptops for those who travel or work from home. The employer has given your spouse rights and permission to use that computer, and you do not have permission to look through it. This is especially important to understand because depending on their occupation, your spouse may have confidential information about their client’s finances, health, legal matters, etc. on their computer. Snooping on a work computer or going through work email is very dangerous because not only are you compromising the privacy concerns of your spouse, but also potentially violating confidentiality of their clients and coworkers.

Guessing a password: You have been married 20 years, you know all of your spouse’s important dates (birthdays, anniversaries, children’s birthdays), you know the name of the street he grew up on, his social security number, the first car he ever drove, and his mothers maiden name. So you start guessing. You either guess the password or are able to correctly answer the security questions and gain access. Simply because you know enough about your spouse to guess their password does not mean you have authorization to log into their computer or email. This would constitute unauthorized access.

Exceeding authorization: Your spouse is at a business meeting, he forgot to bring an important document he was hoping to give to a prospective client. He has a copy of it saved on his work laptop, which is at home. He calls you in a panic asking you to login, find the document, and send it to him; of course he gives you the necessary passwords. Great! Now he is on his way to making that big sale. But now you have the passwords. . . .and he was the one that gave them to you. . .so the next day when he is at the gym you decide you will just take a quick look through his email. In this case, he gave you the password for the limited purpose of sending him that document during his time of panic; that does not mean that he has authorized you to use it again later, for other reasons. If you go looking for incriminating information or emails, you have violated Title II because you have exceeded his authorization.

Authorization can be a tricky thing. If your spouse has given you an email password, or knows that you have it, and knows that you use it, and has not changed it, then you most likely have authorization.

What exactly “unauthorized access” means raises a slew of additional questions: what if there is a folder with all of your spouse’s passwords next to the computer? They haven’t specifically given you access, but you both know where the folder is and what it contains?
What if you were both open with each other about your passwords during your marriage, but then you separate and your spouse fails to change their passwords and then you start snooping? As you can see, unauthorized isn’t quite as straightforward as it seems.

When in doubt, we tell people to ask one question: “Does it feel like an invasion of privacy?”

Because there are not a lot of concrete answers when it comes to “unauthorized access,” positing this question to yourself is a good way to make an initial determination of whether or not you are pushing the boundaries.

**Electronic Communications held in Electronic Storage:**
What exactly this encompasses has been highly litigated, and several clear rules have been defined by the courts. As an initial matter, we should make a distinction between email stored on a computer’s hard drive and emails that are saved in your Gmail account, for example.

If your spouse has physically saved emails to your computer’s hard drive, Title II does not protect these emails. The hard drive is not considered electronic storage.

Similarly, if you use certain Internet Service Providers for email (such as AOL), and the emails are automatically saved to your hard drive, they are also not protected. This tends to seldom be an issue however, because most people use email accounts not furnished by their internet service provider, such as Gmail, Yahoo, Hotmail, and the like.

There has been much litigation concerned with the meaning of electronic storage. The statute defines it as: “any temporary, immediate storage of wire or electronic communications incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”

What is interesting about this definition is that it does not include reference to post-transmission storage, which is where the email would be located after received and opened by the intended recipient.
So does this mean that if your spouse had already opened the email, and it was stored in his Gmail account, it is not protected?

While warranting a complicated analysis, the short answer is no, it is in fact protected. There have been several lengthy and detailed court opinions involving this issue, and ultimately it has been decided that emails, whether opened or not, are protected by Title II.

Another aspect to highlight with regard to the definition of electronic storage is that it limits its protection to emails either (1) stored incidental to transmission or (2) stored for backup protection by the electronic communication service (email provider).

What this means is that if your spouse creates a folder in his email account where he specifically saves incriminating emails, it does not fall under protection. The emails contained in such a folder are not being stored incidental to transmission or for purposes of backup protection by the electronic communication service.

So, oddly enough, while you may not legally have access to the sent mail folder and inbox, you could potentially legally access, without authorization, the folder where he has saved the emails.

Unauthorized access to the folder in which your spouse is manually saving emails is not protected under Title II. Be cautious, just because this type of access is not deemed to violate Title II, it does not mean you are absolved of all legal liability. Your spouse may still be able to sue under the privacy torts we mentioned earlier.

What if I look at my spouse's email on his smart phone, instead of his computer?

The focus of this section has been about email, specifically. Do the rules change with regard to checking your spouse's email on their phone? Checking email on a smart phone usually does not require actually logging in, so it must be different, right?

Authorization is still a key issue. If your spouse is aware that you know the passcode to unlock their iPhone, and that you use their phone from time to time, you probably have authorization to tap that email button and look around.

On the other hand, if you use your detective skills to guess the password, you do not have authorization and you are in violation. Still be wary of looking through work emails on the phone, because the same concerns regarding work email we just mentioned apply to email accessed on a smart phone as well.

Smart phones have undoubtedly added a new layer of complication to this already complex area. Before you act, go back to your instincts and ask yourself, “Does it feel like this snooping is an invasion of privacy?”

Bottom Line: Do not install Spyware on a computer or phone, and do not access your spouse's computer or email without authorization. If it feels like you're invading their privacy, you probably are gaining access illegally.

CAN I SNEAK A PEEK INTO MY SPOUSE’S EMAIL ACCOUNT?
WHAT ABOUT SNOOPING THROUGH MY SPOUSE’S FACEBOOK ACCOUNT?

Can you access this content without being in violation? The same analysis discussed with regard to email applies to snooping on a Facebook account. Some spyware programs will track and record Facebook chats and messages, as well as store passwords to give you easy access. This is unauthorized access, and illegal. If you have authorization, then you are not violating the wiretapping act by logging in and looking around. If you guess a password or correctly answer security questions to gain access, or use spyware, you are unauthorized and in violation.

Public Posts

The information you see on your spouse’s Facebook “timeline” by using your own Facebook account, however, is fair game. Your spouse has no expectation of privacy with regard to information they are putting in a public forum. So if a paramour posts on their timeline, or an incriminating picture appears, you can certainly print it out and bring it to your lawyer. There are some issues regarding the admissibility of Facebook printouts, but those will be discussed in detail later in this article.
CAN I PLACE A GPS TRACKING DEVICE ON MY SPOUSE’S CAR?

Whether it is permissible to place a GPS on your spouse’s car to track their whereabouts is unclear. The Supreme Court had previously determined that, generally speaking, people traveling in vehicles have no reasonable expectation of privacy, and thus one’s whereabouts is not considered confidential information.

However, a recent Supreme Court case regarding the use of GPS tracking devices, U.S. v. Jones, added a new layer of complexity to the constitutionality of using these devices. Jones discussed GPS issues in the criminal procedure arena, specifically whether police officers could use GPS trackers to follow people without warrants.

Some attorneys believe that U.S. v. Jones bans people from using GPS devices to track their spouses, while others believe that U.S. v. Jones is inapplicable because it focuses on police activity. Some attorneys believe that because there is no law specifically prohibiting the use of GPS trackers, it must be legal. And yet other attorneys believe it comes down to ownership of the vehicle, and thus if your name is on the registration and title, then you can use GPS to monitor the vehicle.

While this is not a criminal law article, know that the Supreme Court thinks that the use of a GPS tracker without knowledge of the person being tracked constitutes a trespass. It is possible that courts taking up this question in the family law context may be inclined to feel the same way.

The appellate courts in North Carolina have yet to hear a case involving spouses using GPS trackers. Until then, proceed with caution. It is probably in your best interest to avoid using these devices until there are clearly defined rules. Even though there is no law that specifically bans the use of GPS tracking devices, your spouse could have claims for trespass and invasion of privacy.
If you have stayed with us this far, you are now an expert on what you can and cannot do with regard to snooping through your spouse's phone, email, computer, social media and the like.

Now, how can you use that evidence that you legally discover in court? Do you print out emails and Facebook pages, or do you simply show the judge this information on your phone or laptop?

Our technologically advanced culture has certainly changed the landscape of legal evidence. We now have new types of media that we might want to bring to court, but the question is whether the law lets you use it against your spouse. What do you need to do to make sure the evidence you find is admissible?

There are some basic concepts that may be helpful for you to understand.

1. Authentication

Attorneys must abide by federal or local rules of evidence, depending on where your case is being heard. Often, a major hurdle for attorneys is a concept known as “authentication.” Essentially, when an attorney authenticates a piece of evidence, he or she is proving that the evidence is in fact what it claims to be.

That sounds easy enough: the attorney should easily be able to prove to the judge that the printed emails you provided are in fact emails showing your spouse's adultery, right?

The problem lies in the fact that altering email correspondence is easy to do. You can copy and paste the text of an email into a word document, and then change anything you want.

If your spouse sends you an email and you respond, you can manipulate their original message before you send your reply.

All it takes is a keyboard to change the date, time, or wording of any email before it is printed. Not to mention the fact that it is simple to create an email account using your spouse’s name, so it would appear your spouse was sending messages of a certain nature when in fact the email account does not belong to them.

All these possibilities are why technology has made authentication more difficult.
Here’s what you need to know:

Do not alter emails. You may think it is going to help your case, but remember your spouse will have the opportunity to take the stand and argue that the email has been altered in some fashion. If your spouse has an attorney, the attorney will surely object to emails that they believe have been altered. If the judge believes you have altered emails that you are trying to admit into evidence, it can be fatal to your case.

Provide printouts. While a judge may agree to look at emails you have on your phone or laptop under some circumstances, generally speaking this is a bad idea. When you legally gain access to emails that are pertinent to your case, print them out and provide them to your attorney.

Be prepared to answer questions you feel are unnecessary or self-explanatory. Your attorney will most likely have prepared you for this, but he or she will have to ask you a serious of questions to lay a foundation, under to the rules of evidence, that will “authenticate” the email. You will need to identify the email address of both the sender and the recipient, names in the signature block and subject lines among other details.

Circumstantial authentication. The rules of evidence allow for an email to be authenticated by “appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." Sometimes your attorney will need to authenticate emails by circumstance. For instance, if the email was in the same format as previous emails sent, if it was clear that the email was a reply to a previous email, if the sender, etc. would only know the substance of the email. Your attorney should let you know in advance if he is worried about authenticating emails, and if you'll need to answer questions addressing circumstantial authentication.

Sometimes less is more. Avoid bringing every adulterous email to court. If you have legally obtained the emails, you can provide your attorney with every message you found, but let your attorney pick which ones to use in your hearing. Most family law proceedings have time limits, and it is ineffective to spend so much time showing the judge a bevy of emails that prove an affair. A handful of such emails are probably enough, and your attorney will know which ones are best suited to use in your case.

Be prepared for objections. If you are showing the judge emails that prove your spouse was adulterous, the other attorney will most likely object. Proof of an affair can be of crucial importance in certain family law proceedings, and your spouse's attorney is going to want to keep this kind of evidence out at all costs. Try not to get flustered; your attorney should be prepared to handle the objections.

The same guidelines apply to the admissibility of printouts from social media. With both email and social media your attorney has to prove there exists sufficient confirming circumstances for a jury to believe that the printout is authentic. Absent obvious alterations, judges are typically lenient when it comes to allowing evidence of this nature to be admitted.
Text messages also generally abide by the same authentication rules as emails. If you have a printout or screenshot of exchanged text messages, your attorney will ask how the sender’s name is stored on the phone, what the phone number is, how you know the phone number to be associated with the sender, etc.

Again, it is better to have the text messages converted into tangible form. Showing opposing counsel and the judge the messages on the actual device can be problematic. You certainly want to avoid the text messages being accidently deleted by either attorney or by the judge while you are testifying.

**II. Hearsay**

Another evidentiary issue that can cause complications in admitting email and social media evidence is hearsay. Everyone has heard that word; it is thrown around on every television show and movie that depicts a courtroom scene, and most people think they know exactly what it means. However, hearsay is a very complex evidentiary hurdle that even experienced lawyers sometimes struggle to get past.

Hearsay is a statement that (1) the declarant does not make while testifying at the current trial or hearing; and (2) a party offers in evidence to prove the truth of the matter asserted in the statement.

Generally, hearsay is inadmissible, however there are numerous exceptions and exemptions to hearsay. We won’t get into the nuances of hearsay right now, but know that it can be an obstacle when it comes to getting emails and the like admitted. If your spouse’s attorney objects on hearsay grounds, your attorney should be prepared to respond by either explaining why the email is not hearsay, or how it fits into one of the many exceptions or exemptions to the hearsay rule.
VIOLATIONS: WHAT IS THE WORST THAT CAN HAPPEN TO ME?

So what happens if you are guilty of violating the federal and state wiretapping laws? Violations of these statutes can result in court ordered injunctions, civil damages, and/or criminal penalties.

I. Federal Wire Tapping Act:

**Injunction:** If you are a first time violator of this act, and you have not been found civilly liable for the violation, the court can impose and injunction. This means that you will be forced to cease audio-recordings, remove the spyware from the computer, etc. An injunction will force you to stop violating the law and is essentially a slap on the wrist. This is the least punitive of the possible sanctions.

**Fine:** If you have previously been found in violation of the Federal Wire Tapping Act, the statute provides for a mandatory $500 fine. If you continue to violate the Act, the court can impose a $500 fine for each subsequent violation.

**Imprisonment:** The statute also provides that in lieu of a fine, you can face up to five years of imprisonment.

**Attorney’s Fees:** If found in violation of this, you will have to pay attorney’s fees and general litigation costs of the opposing party.

II. North Carolina Electronic Surveillance Act:

If found in violation of this statute, you are guilty of a Class H Felony.

**Damages:** Compensatory damages are calculated at a rate of $100 per day, for each day in violation, or $1,000 total, whichever is greater. For instance, if you had spyware on your spouse’s computer for one year, the damages could be calculated as high as $36,000. North Carolina’s statute also allows for additional punitive damages, and reasonable attorney’s fees for opposing counsel.

III. Attorney Liability:

If you have obtained information in violation of either the federal or state laws discussed in this article, your attorney may also face liability. A shrewd attorney
Spousal Spying   |   How your online activity is being used against you

will begin questioning you regarding how you obtained the emails, recordings, etc. from the moment you first mention having possession of this sort of evidence.

If the attorney has knowledge that the information was obtained illegally, and looks at it or listens to it any way, he or she is equally liable and faces the same consequences that you may face. Attorneys found in violation of these laws have been criminally fined, placed on probation, forced to temporarily surrender his/her law license, and ordered to pay civil fines as well.

If you walk into your attorney’s office with emails proving your spouse’s adulterous behavior, do not be offended if your attorney immediately questions how the emails were obtained or refuses to read the emails. Your attorney is not being rude by declining to view these emails; he or she is simply absolving himself or herself of liability.

Don’t fret, often there are plenty of other ways to prove an affair without using illegally obtained evidence. Also, keep in mind that evidence of an affair, no matter how earth shattering it is to you, may not make a difference in your case depending on the issues you are litigating.

IV. Destroying Evidence:

This article is written more for a person who suspects a cheating spouse. But what if you are the spouse that cheated, and you know there are emails and Facebook content that can prove your affair? You are worried so you take down your Facebook page, or delete the incriminating content. Or maybe your attorney even suggested that you clean up your Facebook page in anticipation of discovery requests and litigation?

Until recently there has not been much attention given to people who delete, deactivate, or take certain things down from their social media accounts prior to litigation. However, there was a recent case in Massachusetts where an attorney was fined $522,000 for instructing his client to remove photos from his Facebook profile, and the client was fined an additional $180,000 for obeying the attorney. The case did not involve a family law issue, but it is out there and something for both attorneys and clients to be aware of.

Depending on the circumstances, altering your Facebook content could be considered “spoliation of evidence,” which basically means destruction of some kind of material the other side would normally get from you during the course of litigation.

This is a hot topic amongst attorneys right now, especially with regard to family law, because, as we have previously discussed, evidence of an affair can be important.

While we have yet to deal with this specific spoliation issue in North Carolina, attorneys and clients should be mindful of this potential issue and cautious to avoid liability.
COULD I REALLY END UP IN JAIL?

So you know the limits of what you can and cannot do with regard to federal and state wiretapping laws, and what the consequences for both you and your lawyer can be.

You might be wondering if courts really impose these statutory sanctions. Sure, the statute says you can face jail time, but does that really ever happen?

It is unlikely that the federal government is going to bring a case against you for illegal surveillance of your spouse. Their efforts with regard to the wiretapping laws are obviously focused on anti-terrorism, organized crime, drug trafficking, and the like.

However, your disgruntled spouse may press charges, file a complaint against you under either statute, or sue you for common law tort damages. Your spouse may be more inclined to take this action if they are angry or embarrassed that they were caught, if evidence of the affair made a major impact on custody or alimony orders, if you have threatened to sue the paramour, or if they truly felt like their privacy was violated.

In July of 2012 a former Sheriff’s Deputy was forced to defend himself in civil court in Brunswick County, North Carolina for using spyware to monitor his ex-wife’s emails and Internet activity. After hearing only three hours of testimony, a jury awarded a verdict in favor of his ex-wife, and he was ordered to pay compensatory and punitive damages as well as attorney’s fees; the grand total was a whopping $25,400. So think twice before you install that spyware or plant recording devices to catch your spouse in the act, most of the time the consequences outweigh the potential benefit.
What is “Keylogging?”

Keylogging is a term that comes up frequently in North Carolina divorce cases. It can turn a simple case into a complicated federal dispute.

Are you wondering what your spouse is doing on his or her computer? That’s a question that gets asked by most spouses going through a divorce in North Carolina. Keylogging is the tool used by spouses to spy on their spouses use of the computer.

Keystroke logging, otherwise known as “keylogging,” is a way to secretly record each key struck on a keyboard. A person who installs a keylogger on a computer gains access to a plethora of information.

Imagine having access to every single key someone strikes on a computer?

You’d know every movement someone made on a computer from websites visited to login and password information. Essentially the key loggers prevent people from hiding any information.

Even though you clear your Internet history, delete emails, change passwords, etc. the key logger records everything. Once the keylogger records this information, you can structure it so a daily, weekly, monthly, etc. email gets sent to you with all of the recorded information.

Why Would You Use This?

There are several reasons why people are attracted to keyloggers. As a parent it could be incredibly appealing to take comfort in knowing every move your child makes on the computer. Even if you have installed parental control programs that limit website your children can visit, these programs can’t possibly catch everything. A savvy teen can find ways to navigate around these programs, so keyloggers are attractive because they can still give you...
access to what your children are looking at and emailing or chatting about online.

One of the most common uses of keyloggers is in the employment context. Employers use this type of surveillance to monitor what their employees do on work computers. Keeping tabs on the websites your employees are visiting on a work-issued computer is a sure-fire way to make sure they are working as efficiently as possible.

The keylogging use most pertinent to this article is spouse-surveillance in North Carolina. What if you suspect your spouse might be having an affair? Maybe you have access to his email account but he's smart enough to delete those incriminating emails?

A key logger still records all of the keys he strikes on that keyboard, so you would still have access to the content of those emails. The key logger also records the keys he strikes while he logs into financial institutions.

Imagine that your husband has a secret bank account? Maybe he's using that money to purchase his mistress meals, take her on vacation, and buy her lingerie? Key loggers give you access to all of this information.

**HOW DOES IT WORK?**

There are two types of keyloggers; they can either be software-based or hardware-based.

**Software-Based Keyloggers**

Software-based keyloggers target a computer’s actual operating system and can even be attached to a computer remotely; it is a type of spyware. There are various different types of software keyloggers that achieve the same goal through different methods. The different types are known as hypervisor-based, kernel based, API based, form grabbing based, memory injection based, and packet analyzers. Without getting into the complex details of what distinguishes these various types of keyloggers, it is worth noting just how many different types there are.

Remote software keyloggers can be used to access someone’s computer from afar, without their knowledge.

Some computer viruses, like the infamous Trojan Horse, use remote software keylogging technology to maliciously and surreptitiously steal sensitive information. Once the Trojan Horse is remotely enabled on a computer it allows access to all sorts of sensitive information. These viruses that use keylogging technology are frequently referred to as “malware.” Interestingly enough, private individuals wishing to monitor a spouse’s computer activity can do so using the same technology that allows hackers to steal confidential information.

Remote keyloggers may be especially attractive to a spouse who suspects a workplace affair. This technology allows you to “bug” your spouse’s
office computer without you even needing to lay eyes on the computer or gain access to the office.

**Hardware-Based Keyloggers**

This type of keylogger can capture the same type of information that a software keylogger can, but it does so via a different method. To enable a hardware-based keylogger one must use something called a “BIOS-level firmware” or plug a device into the computer. These devices intercept and record keystroke data. Rather than receiving emails reporting on the computer activity, installers of hardware-based keyloggers gain access by typing a special password into a text editor on the computer. A correct password will generate a menu allowing the installer of the keylogger to navigate the recorded computer activity.

There are several versions of hardware based-keyloggers. Some look like jump drives that plug into USB ports, others can retrieve information from wireless keyboards, some use firmware, and there are even keyboard overlays.

**Pros and Cons**

1. **Accessibility:** Software-based keyloggers are especially attractive to those who wish to spy on a computer remotely. For instance, a curious husband can remotely monitor his wife’s activity on her office computer, or a parent can use this to remotely gain access to their child’s laptop.

Hardware-based keyloggers require physical access to the computer somewhat frequently. You will need access to install it, and again each time you will want to retrieve information. So this might be a good option for a home computer, but not practical if you want to monitor a computer you cannot easily access.

2. **Countermeasures:** Users of software keyloggers can easily be halted by anti-keylogging software designed to detect and alert a user of the existence of the keylogger.

Some prefer hardware-based keyloggers precisely for this reason – they cannot be thwarted by anti-keylogging software. Because hardware keyloggers refrain from interfering with the operating system, they are not detectable by anti-keylogging software. The only way to prevent someone from using one of these is to simply deny physical access to the computer or visually inspect the computer before using it.

**WHERE CAN I GET A KEYLOGGER?**

A quick Google search can pull up countless products, and they are fairly inexpensive. For instance, you can purchase remote keylogger software from “Keylogger Pro” for a mere $39.99. This product’s advertising boasts that it can record keystrokes on any keyboard, even foreign
keyboards. Not only does this remote key logger record keystrokes, it can also provide high-resolution screen shots of user activity. Hardware keyloggers sold on amazon.com range in price from $33 to $180.

Keyloggers.com is a website solely devoted to helping you find the best keylogger for your needs. Here you can find user reviews, pros/cons of various keylogging products, pricing, and very detailed explanations of exactly what each product is capable of.

As you can see, these programs and devices are easy to purchase, fairly inexpensive, and can give you access to all sorts of information.

ARE KEYLOGGERS LEGAL?

1. Federal Law

There are two federal laws that could potentially be implicated with regard to keyloggers, and the legality of these programs and devices has been the topic of some recent litigation.

Title I of the Electronic Communications Privacy Act

Title I of the Electronic Communications Privacy Act ("ECPA") provides specifically that one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication" faces both criminal and civil liability. The important most important word in this definition arguably being "intercept;" interception must be contemporaneous with transmission.

Title II of the Electronic Communications Privacy Act

Title II of the Stored Wire and Communications Act imposes criminal and civil liability to those who intentionally gain unauthorized access to electronic communications held in electronic storage.

II. North Carolina Law

The North Carolina Electronic Surveillance Act provides much of the same information as Title I of the federal law we just mentioned. It
prohibits interception of wire, oral, or electronic communications. The same issues with interception being contemporaneous with transmission exist when applying this law to keylogging.

North Carolina also has laws regarding computer-related crimes that prohibit unlawful access to another person's computer, system, program, or network without authorization. This most closely mirrors Title II of the federal law.

Additionally, you need to be aware that North Carolina recognizes several privacy tort claims that may also apply. “Intrusion upon seclusion,” which is a fancy way of saying invasion of privacy, is recognized in North Carolina as grounds for a lawsuit. North Carolina also recognizes other torts that could apply depending on the situation, including trespass and intentional or negligent infliction of emotional distress.

**HOW DOES THIS PLAY OUT IN REALITY?**

In 2011 an Indiana woman sued her employer for using a software-based keylogger to access her emails and personal checking account information. She unsuccessfully argued that her employer violated Title I because they intercepted her keystrokes, which ultimately gave them access to her email and bank account login information and content. The court focused on the requirement of interception being contemporaneous with transmission, and in this case found that the Indiana woman failed to prove that the sensitive information was in fact recorded contemporaneous with transmission.

The court went one step further and also found that typing on a keyboard did not constitute electronic communication. The statute specifically describes such communication as that affecting interstate or foreign commerce. The court opined that because the software didn’t transmit the recorded keystroke information beyond her office computer, there was no way interstate commerce could have been affected.

Courts have struggled with the concept of interstate commerce and its application to the definition of electronic communication. Some have found that if the computer is connected to a modem and a network that is enough to satisfy an affect on interstate commerce. Other courts have disagreed completely with this analysis.

A 2013 North Carolina case disagrees with the ruling in the Indiana case mentioned above. That opinion specifically states that the interpretation of electronic communication used previously was too narrow. Here the judge explained that the whether there was an affect on interstate commerce should be with regard to the content of the actual communication, and not the way it was intercepted.

While courts have been reluctant to find that keyloggers violate Title I of the ECPA, the future is uncharted territory. Last month’s opinion could indicate a shift in federal court’s attitude towards keylogging, but as it stands it seems hard to be found to have violated Title I by using a keylogger.
In the case of the Indiana woman discussed above, while her Title I claim was unsuccessful, her Title II claim was preserved. If it can be proven that the keylogger allowed an individual unauthorized access to electronic communications held in electronic storage, that individual has violated Title II via the keylogger.

The problem with applying Title II to keyloggers, is that courts have been all over the place with regard to how to treat emails whose content was obtained through use of a keylogger. There is conflicting opinion as to whether it matters if the emails had been opened and whether they were stored manually or saved by the Internet service provider.

**SO ARE THEY ILLEGAL OR NOT?**

There exist numerous law review articles devoted to the need for reform in this area. There have been several proposed spyware bills that have attempted to address the lack of consistency with regard to keyloggers and loopholes that currently exist. The reality is that as it stands, there are gaps in Title I and Title II, and a myriad of conflicting opinions, which make the question of federal liability unclear.

Our advice is to proceed with caution. This is an area of the law with a lot of unknowns. With regard to federal law, the answer to the question of the legality of keyloggers is very unclear. Some courts read the statutes narrowly, others more broadly. Until there are clearly defined rules, either through judicial opinions or legislation, it is unclear whether use of a keylogger will result in liability under Title I or Title II.

Even if you aren’t found to have violated a federal law, you can still be found guilty of violating the state law addressing computer related crimes, and you may face liability with regard to common law tort claims.

Because use of keyloggers can implicate several state and federal laws, we advise you to stay away from using keyloggers to catch your spouse in the act of cheating.
The Electronic Communications Privacy Act and the Stored Wire and Electronic Communications Act, commonly lumped together as the Electronic Communications Privacy Act (“ECPA”), are federal laws that prohibit certain types of electronic eavesdropping. Congress enacted these laws in 1986 to update the Federal Wiretap Act of 1968. The original ban on wiretapping protected a person’s privacy while using telephone lines. The 1968 legislation did not envision the use of such modes of communication as electronic messages, Internet chat rooms, text messaging, cellular telephones, Internet bulletin boards, or voice over IP. Since the ECPA was enacted, it has also been updated to reflect new technology. The ECPA created penalties for any person who intentionally 1) intercepts, uses or discloses any wire or oral communication by using any electronic, mechanical, or other device, or 2) without authority accesses a wire or electronic communication while in storage. A distinction is made between the “interception” of electronic communications and mere access to communications that are in “storage.” The legislative intent was to provide stiffer penalties for “interception” than for accessing communications in “storage.” The statute defines “interception” as the “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Electronic storage is “any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”

WHAT TYPES OF COMMUNICATIONS ARE COVERED?

The law applies to traditional telephone wiretaps, cordless telephone interceptions, electronic messages, voicemail systems, pagers, chat logs, web-streaming video, voice over IP, and recording or videotaping private face-to-face conversations. This list is not exhaustive but provides a hint of the wide-ranging application of this law to many types of communication.

WHAT IF MY SPOUSE GAVE ME ACCESS TO HIS/HER EMAIL ACCOUNT AND PRIVATE CHAT ROOM?

Consent is another principle to consider when deciding whether the ECPA applies. The ECPA only prohibits “unauthorized” use, disclosure, or interception. If your spouse has routinely given you his email account passwords and allowed you to use them, he has authorized you to find what you will. The courts will decide this issue of consent on a case-by-case basis, and it is not necessary for consent to be explicit. Implied consent can be found when the surrounding circumstances are taken into account. In light of the complexity of this area of the law, it is advisable for you to consult an attorney before taking any action that might be considered in violation of the ECPA.
WHICH TELEPHONE CALLS CAN I RECORD?

Under the North Carolina statute, it is permissible to record a phone conversation if one of the parties to the communication is aware of and has consented to its being recorded. This means that you can record your own telephone calls. On the other hand, it is illegal to record telephone calls between your spouse and a third party, if neither party knows that the conversation is being recorded. It is important to be aware that some states require that both parties to a telephone call be aware of and consent to its being recorded. If you are recording a telephone call, and one of the callers is out-of-state, you could be violating the law of that state.

MY SPOUSE PREVIOUSLY GAVE ME HIS EMAIL PASSWORD TO RETRIEVE AN ELECTRONIC BILL; CAN I USE IT TO SEE WHAT HE IS UP TO NOW THAT WE ARE SEPARATED?

The question here is whether your spouse gave up his or her expectation of privacy in this email account when he or she gave you the password. The ECPA envisions this type of privacy intrusion by prohibiting not only the unauthorized access to stored communications, but by also prohibiting the access of stored communications by one exceeding her authority. In practice, this means that if the password was given to you for a certain purpose, you could not use it for other purposes. To do so could expose you to financial and criminal consequences.

CAN I READ MY SPOUSE’S EMAIL MESSAGES?

This question depends on several factors. First, how did you obtain the information? If it was unintentional, you may use it any way you please. The ECPA only prohibits the intentional interception or unauthorized access to electronic communications. Therefore, if a message is sent to you in error, you may use the contents in any manner that you see fit. However, a password is required to access most email programs. If you have improperly obtained your spouse's password, it would be illegal to access the messages. Should you acquire electronic communications that are stored, rather than intercepting communications as they unfold, you may use the information you obtain. Most importantly, it may be used as evidence in your divorce. In addition, you may disclose it to others. However, you should be aware that by doing so, you may be exposing yourself to a lawsuit or criminal charges. Whether your individual situation could expose you to the penalties of the ECPA is a fact-specific inquiry. Therefore, it is advisable to obtain the advice of an attorney before taking any action.

WHAT ARE THE PENALTIES FOR VIOLATING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)?

There are both civil and criminal penalties for a violation of the ECPA. It can be very financially damaging if you are found in violation of this law. For example, a court can award damages to the victim of such eavesdropping. The damages are calculated in a way that each day of continuation of the violation gives rise to a higher amount of damages. In addition, the court can force you to pay the attorneys’ fees of the
other party, which could be higher than the amount of damages. A court may also impose additional, punitive damages if the violation is especially malicious. Finally, a court may impose a term of imprisonment not to exceed five years for a violation of the ECPA. In addition to the federal law, there are also state laws affecting your ability to engage in electronic eavesdropping. North Carolina General Statute Section 15A-287 criminalizes the willful interception, use or disclosure of the contents of any wire, oral, or electronic communication “without the consent of at least one party to the communication.” This has been categorized as a Class H felony. As if the foregoing penalties are not enough deterrent, you could also be sued under North Carolina common law for an “invasion of privacy.” Again, this could expose you to similar economic damages.

WITH SUCH A CONFUSING AREA OF THE LAW, HOW CAN I KNOW WHAT IS PERMISSIBLE AND WHAT IS NOT?

The law of privacy in electronic communications is notorious for its lack of clarity. This is evidenced by the lack of a uniform interpretation of this law by the various federal courts. However, there are some general guidelines to keep in mind when faced with the question of whether you are committing a violation of the ECPA. The first and most basic principle underlying this law is the concept of a “justifiable expectation of privacy.” A justifiable expectation of privacy must accompany the communication in order for a violation of the ECPA to occur. In most cases, it is not hard to imagine which communications involve an expectation of privacy exists. For example, a reasonable person is justified in expecting his/her telephone calls to be private. However, a reasonable person would not consider a message placed on a bulletin board in the county courthouse to be private. This principle can be extended to each type of electronic communication. Most people would consider an email message to be private. The software for accessing such messages requires a password, which is a good indication of the expectation of privacy. However, a joint email account where spouses share the service and are both aware of the password, would probably not be deemed to be private. Another gray area in applying this law concerns chat rooms. Many chat rooms are restricted to those who “register” for the service. However, the fact that access is limited to those who register does not necessarily mean that the discussions are justifiably expected to be private. On the other hand, some chat rooms are private and only available to those with a password.

I AM WORRIED ABOUT WHAT MY SPOUSE IS SAYING TO MY CHILD WHEN THEY TALK ON THE PHONE; CAN I RECORD THEIR CONVERSATIONS?

The 6th Circuit Court of Appeals (which is not the Circuit Court of Appeals governing North Carolina) has found that a parent may consent for a child’s conversation to be recorded. The Court required that the parent consenting for the child present a good faith, objectively reasonable basis for believing such action was necessary for the welfare of the child. However, there is no similar rule in effect for the 4th Circuit Court of Appeals, which includes North Carolina. The taping of such a conversation would be a violation of the ECPA. It is clearly an illegal interception of a communication using a device, which would put it squarely within the prohibitions of the ECPA. Taping a child’s telephone conversation...
with the other parent would also violate North Carolina state criminal law (G.S. 15A-287). However, it is not illegal to use another phone in your home, in the ordinary course of business, to listen in on the conversation. This is referred to as the “extension line” exception to the ECPA. It is based on the principle that it is not illegal to monitor a conversation that one could otherwise hear legally. There is a conflict of opinion in the federal courts on whether you can record such a conversation. To do so is at your own risk of being found in violation of the ECPA.

IF I TAPED MY SPOUSE’S TELEPHONE CONVERSATION ILLEGALLY, WHAT CAN I DO WITH THE INFORMATION I OBTAIN?

This is where the distinction between “interception” and “accessing a stored electronic communication” becomes critical. If you placed a wiretap on a telephone, or hired a computer professional to break into your spouse’s computer to monitor his chat room discussions, this is obviously an “interception.” Some courts have defined interception to mean acquiring communications as they are transmitted. If you have intercepted a message, you may not use it for any purpose. You may not tell anyone else the contents of it, even by paraphrasing. You may not use it in evidence in your divorce. Each instance of disclosing the information to another person can theoretically be considered a separate cause of action for damages or criminal culpability. One federal court has found that even those who listen to the illegally recorded conversations can be found liable for violating the statute.

HOW CAN I PROTECT MYSELF FROM UNWANTED INTRUSIONS INTO MY OWN ELECTRONIC PRIVACY?

The Internet is inherently susceptible to surveillance by private individuals who are willing to put forth the expense and effort to do so. However, it is possible to place hurdles in the way of individuals without the technical knowledge to hack into your computer. Such steps include installation of firewall software, password protection, and encryption software. Firewalls help prevent unwanted access and unsolicited scans coming form the Internet. Password protection is available on all email programs. Encryption software is an effective method of sending and storing electronic messages in a format that is illegible to someone without “decrypting” software. Should you discover that you have been the victim of an ECPA violation, you have legal recourse. You may file a lawsuit for injunctive relief (i.e. to stop the intrusion), actual damages, punitive damages, and attorneys' fees. You are required to file such a lawsuit within two years after the date upon which you had a reasonable opportunity to discover the violation of the ECPA. The other legal actions available to you are criminal charges and a civil lawsuit for invasion of privacy under North Carolina law.
THE LAW: STATUTES AND CASES
Here you will find a list of statutes and cases that are applicable to Spousal Spying.

I. FEDERAL STATUTES

18 U.S.C. § 2510 – Relevant Definitions

(1) “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 between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) “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;

(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. [1]

(5) “electronic, mechanical, or other device” means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—

   (a) any telephone or telegraph instrument, equipment or facility, or any component thereof,

      (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

      (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

   (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(12) “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 that affects interstate or foreign commerce, but does not include—

   (A) any wire or oral communication;
(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) “readily accessible to the general public” means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) “electronic storage” means—

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

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;
18 U.S.C. § 2511 – Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

   (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

   (b) 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 when—

      (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

      (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

      (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

      (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

   (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; or

   (e)

      (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511 (2)(a)(ii), 2511 (2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter,
(ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation,

(iii) having obtained or received the information in connection with a criminal investigation, and

(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(4)

(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.
18 U.S.C § 2701 – Unlawful Access to Stored Communications

(a) Offense.— Except as provided in subsection (c) of this section whoever—

(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 shall be punished as provided in subsection (b) of this section.

(b) Punishment.— The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph;

and

(2) in any other case—

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

II. N.C. STATUTES

N.C. Gen. Stat. § 14-458 – Computer Trespass; Penalty

(a) Except as otherwise made unlawful by this Article, it shall be unlawful for any person to use a computer or computer network without authority and with the intent to do any of the following:
(1) Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network.

(2) Cause a computer to malfunction, regardless of how long the malfunction persists.

(3) Alter or erase any computer data, computer programs, or computer software.

(4) Cause physical injury to the property of another.

(5) Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.

(6) Falsely identify with the intent to deceive or defraud the recipient or forge commercial electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk commercial electronic mail through or into the computer network of an electronic mail service provider or its subscribers.

For purposes of this subsection, a person is “without authority” when (i) the person has no right or permission of the owner to use a computer, or the person uses a computer in a manner exceeding the right or permission, or (ii) the person uses a computer or computer network, or the computer services of an electronic mail service provider to transmit unsolicited bulk commercial electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider.

(b) Any person who violates this section shall be guilty of computer trespass, which offense shall be punishable as a Class 3 misdemeanor. If there is damage to the property of another and the damage is valued at less than two thousand five hundred dollars ($2,500) caused by the person's act in violation of this section, the offense shall be punished as a Class 1 misdemeanor. If there is damage to the property of another valued at two thousand five hundred dollars ($2,500) or more caused by the person's act in violation of this section, the offense shall be punished as a Class I felony.

(c) Any person whose property or person is injured by reason of a violation of this section may sue for and recover any damages sustained and the costs of the suit pursuant to G.S. 1-539.2A. (1999-212, s. 3; 2000-125, s. 7.)
III. RELEVANT CASES

The following cases, listed in alphabetical order, have shaped the way that courts have approached violations of state and federal wire tapping laws.

Finding emails stored on the hard drive of a computer does not constitute “interception” and thus does not violate the ECPA. Interceptoin occus contemporaneously with transmission.

There is no inter-spousal exception to the Federal Wiretapping act.

Kee v. City of Rowlett, 247 F.3d 206 (11th Cir. 2001)
Applies “reasonable expectation of privacy to the Wiretapping Act.

One must demonstrate that they had an actual expectation of privacy with regard to the material in question, and also that expectation of privacy is one that society recognizes as reasonable.

Because North Carolina is a one-party consent state, a wife violated the law when she placed a voice-activated recording device in the marital home and recorded her husband’s conversations with others. The wife could not consent to this as she was not a party to the conversations.
The Federal and State wiretapping laws only apply to oral communications. Video recording a spouse does not violate the ECPA unless the videotaping also inclues an audio recording.
Pollock v. Pollock, 154 F.3d 601 (6th Cir. 1998)

⇒ The court determined that it was permissible for a mother to tape record her daughter’s phone calls with her father despite the fact that none of the parties had consented.
⇒ As long as there is a “good faith basis” for recording the conversation (i.e., emotional abuse), vicarious consent can be established.


⇒ North Carolina is a one party consent state; interception of phone calls does not violate the ECPA as long as at least one party consents to the communication.
⇒ Because both parties heard a warning on the telephone that the call was being recorded, and they continued to speak, consent to the recording was implied.

U.S. v. Steiger, 318 F.3d 1039 (11th Cir. 2003)

⇒ Intercepting an email contemporaneously with transmission is virtually impossible unless some type of automatic routing software is used.

Vieux v. Pepe, 184 F.3d 59 (1st Cir. 1999)

⇒ Vicarious consent arises out of parental concern and is not “so close a question as one that fell within the scope of Congress’s concern about evidence from wiretaps being used in marital disputes.


⇒ Wife had “authorization” to access husband’s email because she had authority to use the family computer and subsequently accessed emails stored on the hard drive that husband had failed to take steps to protect.