Digital Espionage in Matrimonial Cases: Drawing the Line Between Legitimate Self-help and Unlawful Interception of Electronic Communications

by
Nicholas G. Himonidis*

Introduction

"*It is appallingly obvious that our technology has exceeded our humanity*." The source of this 'infamous' quote (often attributed to Albert Einstein) is uncertain. This much is certain: matrimonial litigants often convince themselves that the key to a successful outcome is getting their hands on their spouse's data, particularly emails, texts, and other electronic communications. In an alarming number of cases, both reported and unreported to which this author can attest, parties utilize a wide range of methods from hacking of email accounts, setting up auto-forward rules, or accessing the spouse's iCloud through a separate (sometimes a child's) device, to the installation of spyware programs on devices used by their spouse. Although there are certain, *limited circumstances* in which the exercise of "self-help" to collect Electronically Stored Information ("ESI") outside of formal discovery by a spouse in a matrimonial case may be legal, much of the conduct described above, which this author has investigated on occasions too numerous to count, violates state and federal criminal statutes, gives rise to statutory claims for civil damages, results in evidence that is inadmissible by statue or case law, and

* Attorney at Law, Licensed Private Investigator, Certified Computer Forensic Specialist, Certified Fraud Examiner, Certified Cryptocurrency Forensic Investigator, Court Qualified Expert Witness in Digital Forensics and the Authentication of Digital Evidence, Founder & President, The NGH Group, Inc., Melville, New York.

can also result in direct and serious sanctions against the offending spouse in the matrimonial action itself.

This article will discuss the various state and federal laws that criminalize electronic hacking and surveillance and give rise to the other liabilities and sanctions mentioned above. The article will also discuss the limited circumstances in which "self-help" may be legal – and attempt to distinguish those situations from the unlawful interception of ESI in the form of electronic communications under applicable law. Section I explores the reasons why parties to matrimonial cases engage in this conduct, and why, in the author's opinion, there has been such a dramatic rise in the frequency of this conduct, and the number of cases dealing with this issues in recent years. Section II sets forth the statutory prohibitions under both federal and many state laws, which criminalize much of this conduct, provide statutory civil rights of action for damages to victims of this conduct, and discusses the issue of whether evidence obtained in contravention of these statutes may still be admissible. Section III presents what the author believes to be a novel case in which a matrimonial court, faced with evidence of digital spousal espionage including the interception of electronic communications, and evidence of spoilation which the court concludes was designed to cover up the misconduct, issued the ultimate sanction against the 'guilty' party and dismissed their pleading(s). In Section IV we distinguish between lawful, legitimate self-help by a spouse in gathering ESI outside of formal discovery – and conduct that violates the statutes discussed in this article, and potentially others, often with drastic consequences. In the Conclusion, we restate the key point of this article – that intercepting the electronic communications of your current or estranged spouse (or anyone else), without the consent of at least one of the parties to the communication, is criminal, sanctionable, gives rise to monetary damages, and usually results in evidence that is inadmissible. We conclude by suggesting in the strongest possible terms, that since the number of cases involving this conduct are sharply on the rise (as a result of the relative ease with which it can be done using modern technology) that matrimonial attorneys would be doing their clients a tremendous service by affirmatively counseling them at the outset of a representation regarding the myriad of

legal consequences for this conduct, and to convince them, wherever possible, that the end certainly does not justify the means.

I. Why Do They Do It?

The emotional motives of adverse litigants is nowhere more prevalent than in matrimonial (and custody) cases. In the author's experience, however, most of the individuals who engage in electronic surveillance conduct are searching for evidence they believe will give them a legal or strategic advantage in their pending or soon to be filed case. Relevant "evidence" is any information which tends to prove or disprove a fact in controversy. By the year 2007 almost 95% of the information in the world was created and stored digitally.[1] What follows is that 95% of potential evidence exists in digital form – *and a great deal of that evidence exists only in digital form*.

Increasingly, businesses and households have gone totally "paperless" – never generating a paper record of a transaction – or destroying the paper records once they are saved electronically. Personal computers, smartphones, tablets and "smart watches" are everywhere. Emails and "texting" (including SMS, iMessage, and messaging through platforms like WhatsApp), along with messaging through social media platforms, has largely replaced telephone (and in person) conversation as the predominant mode of business and personal communication. These are the realities of modern society.

More than 80% of Americans own a "smartphone."[2] People carry them and use them almost everywhere they go, creating digital breadcrumbs to their whereabouts and activities. Almost 90% of Americans with bank accounts access those accounts online at least sometimes; and almost 70% of them manage their bank accounts primarily or exclusively online.[3] Virtually every bank and credit card company now offers a "paperless" option to

---

1 Rebecca Boyle, *All the Digital Data in the World Is Equivalent to One Human Brain*, Popular Sci. (Feb. 11, 2011), https://www.popsci.com/technology/article/2011-02/new-study-inventories-all-data-world-and-measures-how-its-stored-and-shared/.

2 *Internet & Technology Mobile Fact Sheet*, Pew Research Center (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/.

3 I. Mitic, *Everything You Need to Know About Online Banking: Statistics and Facts*, Fortunly (Apr. 30, 2020).

their customers. Once enrolled, the customer never again receives any paper statements or transaction records.

Bitcoin (BTC) and other cryptocurrencies have become mainstream investments – but they are also commonly used as vehicles to hide funds and conduct anonymous transactions. As of this writing, nearly $27 billion worth of BTC changes hands every day.[4] There is literally no paper trail when BTC transactions are done peer-to-peer (i.e. without the involvement of a broker) and there is no one upon whom to serve a subpoena for information about such transactions.

Facebook had over 256 million monthly active users in the United States (and Canada) in the second quarter of 2020.[5] There are more than 48 million active Twitter users in the United States[6] – contributing to an average volume of more than 500 million Tweets per day worldwide.

Desktops and laptops with hard drives of multiple terabytes are now commonplace in homes. A one terabyte hard drive can store more than 100 million pages of text, millions of emails, over 300,000 digital photos, 1,000 hours of digital video footage – or any combination of the same as well as other forms of ESI too numerous to list.

There is certainly good reason for litigants and their counsel to seek out this evidence. Unfortunately, a disturbing trend has developed whereby parties are taking matters into their own hands. Without proper advice from counsel, or the assistance of knowledgeable professionals, these parties will often utilize methods suggested to them by well-meaning friends, "the IT guy at work," or which they discover online, to engage in all manner of digital espionage. When the conduct and methods are limited to accessing and/or copying STATIC ESI from computing devices or data stores in the marital home, this conduct may be permissible. When it crosses the line to the interception of electronic

---

4 CoinMarketCap.com, https://coinmarketcap.com/ (last visited Nov. 15, 2020) listing the top 100 cryptocurrencies, their current market price, market cap, circulation and 24 hour trading volume.

5 www.statista.com/statistics-number-of-monthly-active-facebook-users-worldwide

6 Omnicore: Twitter by the Numbers: Stats, Demographics & Fun Facts; (Feb. 10, 2020).

communications "in transit" however, it is almost always unlawful and there can be severe criminal and civil consequences.

It is essential for matrimonial attorneys to be aware of the frequency with which this occurs, and to counsel clients early, and often, regarding the serious consequences that can result from crossing the line between legitimate "self-help" and unlawful interception.

II. Statutes Prohibiting Interception of Electronic Communications

Title 18 of the United States Code, covering federal crimes and criminal procedure, may seem an unlikely place to begin a discussion of conduct engaged in by parties to matrimonial litigation. It is, however, at the very core of this topic. The Omnibus Crime Control and Safe Streets Act of 1968 as updated and amended by the 1986 Electronic Communications Privacy Act[7] (the "ECPA") expressly prohibits the interception of wire, oral or electronic communications.[8] It also expressly prohibits the disclosure or "use" of any such intercepted communications.[9] The ECPA defines "electronic communication" as "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."[10] In short, all forms of modern communication fall under the ECPA prohibitions on interception, including phone calls, emails, social media messages, and all forms of text messages.[11]

Interceptions violate the provisions of the ECPA if done without the knowledge and consent of at least one party to the

---

7 18 U.S.C. §§ 2510-2523 (2018).

8 18 U.S.C. § 2511(1)(a).

9 18 U.S.C. § 2511(1)(c)(d).

10 18 U.S.C. § 2511(12). However, the definition 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.

11 18 U.S.C. § 2511(1)(a).

communication[12] and violators are subject to incarceration for up to five (5) years and fines of up to $10,000 *per violation*.[13] In addition, the ECPA provides a direct civil right of action by victims against violators, with civil penalties including (i) actual damages capped at $1,000; (ii) punitive damages; and (iii) reasonable attorney's fees and other litigation costs.[14] While federal criminal prosecutions under the ECPA arising out of matrimonial cases are rare, civil cases arising from matrimonial fact patterns seeking damages under the private right of action provisions of the ECPA are not. Examples as far back the early 1970's are cited and discussed below. Early cases dealt with the unlawful interception (and recording) of phone calls (since email, texting, and social media did not exist at the time) but the provisions of the ECPA relevant to this discussion are the same (with the exception of provisions of the ECPA dealing with suppression that distinguish between oral and wire, and electronic communications).[15]

Section 2511 of the ECPA provides as follows:

> (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;
>
> . . .

---

12 18 U.S.C. § 2511(2)(d): "It shall not be unlawful under this chapter [§§ 2510-2520 of this title] for a person not acting under color of law to intercept a wire or oral 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 unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act."

13 18 U.S.C. § 2511(4)(a).

14 18 U.S.C. §2520(b)(1)(2)(3).

15 *See* 18 U.S.C. § 2515 (emphasis added): "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 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."

> (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; . . .
>
> . . .
>
> (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.

Many states have penal statutes that are modeled after the ECPA (or its predecessor, the 1968 Act),[16] or which in some fashion prohibit the same conduct.[17] New York Penal Law Article 250, the New York "Eavesdropping Statute," for example, pre-dates the ECPA (and the 1968 Act) but criminalizes the interception of electronic communications as follows: "A person is guilty of eavesdropping when he unlawfully engages in wiretapping, mechanical overhearing of a conversation, *or intercepting or accessing of an electronic communication*. Eavesdropping is a class E felony."[18] The New York Penal Law defines an "electronic communication" as "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 photo-optical system."[19] Just as with the ECPA, "electronic communications" clearly encompasses email, any form of text message, and/or any form of direct social media messaging under the New York Penal Law.[20]

---

16 *E.g.*, N.J. STAT. § 2A:156A-2.

17 *E.g.,* CAL. PENAL CODE § 637.2 (2019) (Invasion of Privacy); CONN. GEN. STAT. § 52-570d (2019) (Action for Illegal Recording of Private Telephonic Communications); FLA. STAT. § 934.27 (2019) (Security of Communications; Surveillance); 720 ILL. COMP. STAT. § 5/14-2 (from ch. 38, ¶14-2); MASS. GEN. LAWS ch. 272, § 99 (2019) (Interception of Wire and Oral Communications); N.Y. PENAL LAW § 250.05 (Eavesdropping).

18 N.Y. PENAL LAW § 250.05 (emphasis added).

19 N.Y. PENAL LAW § 250.00(5).

20 *See generally* CC V. AR, 100 N.Y.S.3d 609 (N.Y. Sup. Ct. 2018).

The ECPA, and many of the state penal statute corollaries, make it a criminal offense for a spouse to intercept the text messages, emails or other electronic communications of the other spouse without consent, and some, including the federal statute, also *criminalize the dissemination or "use"* of any such intercepted communications, either by the interceptor *or any other person*, provided that the user or disseminator knows the source of the material in question.[21] These provisions make it absolutely essential for matrimonial counsel to know exactly how their client acquired something that purports to be the other party's phone call(s), email(s) or text message(s) – lest counsel find themselves on the wrong side of a "United States v." or "People v." suit – or named as a defendant in a state or federal civil suit for damages under the private right of action under the ECPA or one of its state law corollaries.[22]

Nowhere in the ECPA does it state – or imply – that any exception exists for a spouse who engages in the proscribed conduct within the marital relationship, within the marital home, or in connection with a matrimonial proceeding (absent consent of one party to the communication). It is simply not there. Nonetheless, there is a line of cases starting with *Simpson v. Simpson* in 1974,[23] that erroneously read such an implied exemption into the ECPA. *Simpson* was followed by other federal and state court decisions for a time,[24] but this line of cases – and its faulty reasoning – has been abandoned and no recent cases seem to follow this outdated and erroneous holding.

In 1974 the issue facing the Fifth Circuit Court of Appeals in *Simpson* was whether the interception by a husband of his wife's conversations with a third party over the telephone in the marital

---

21 18 U.S.C. § 2511(1)(c); 720 ILL. COMP. STAT § 5/14-2(3) (Illinois Wiretapping Statute); N.H. REV. STAT. ANN. ch. 570-A (New Hampshire Wiretapping and Eavesdropping Statute); 18 PA. CON. STAT. ANN. §§ 5701-5781

22 *See, e.g.,* Zaratzian v. Abadir, No. 10-cv-9049, 2015 WL 5474246 (S.D.N.Y. July 8, 2015), *aff'd*, No. 15-1243-cv (2d Cir. May 26, 2017) (the husband's attorney was named as a defendant along with the husband, where the husband provided to the attorney, and the attorney received and used the emails the plaintiff's wife alleged that the husband had intercepted in violation of the ECPA).

23 490 F.2d 803 (5th Cir. 1974).

24 Stewart v. Stewart, 645 So. 2d 1319 (Miss. 1994); Baumrind v. Ewing, 279 S.E.2d 359 (S.C. 1981); Beaber v. Beaber, 322 N.E.2d 910 (Ohio 1974).

home violated the ECPA. The husband suspected his wife of being unfaithful and obtained a device for tapping and recording telephone conversations and deployed it within the marital residence, intercepting and recording conversations between his wife and another man. Using the recordings as leverage, Mr. Simpson convinced his wife to agree to an uncontested divorce. Mrs. Simpson sued Mr. Simpson in federal district court seeking civil damages under the ECPA.[25] The district court found that the interception by a husband using electronic equipment of the conversations between his wife with a third party over the telephone in the marital home was not covered under the ECPA.[26] Mrs. Simpson appealed.

After what the Fifth Circuit described as "an independent search of legislative materials regarding the ECPA," which the court referred to as "long, exhaustive and inconclusive,"[27] the court held that Congress did not intend for the ECPA (despite its inclusive language) to extend to cases involving a husband and wife.[28] The court stated that it found due to "inconclusive legislative history" that Congress did not intend to prohibit a person from intercepting a family member's telephone conversations by use of an extension phone in the family home.[29] The holding in *Simpson* was an egregious example of a court ignoring the plain meaning of an unambiguous and inclusive statute, inserting instead its own meaning based on what the court apparently felt was the proper result from a policy standpoint.

Because many state statutes prohibiting this conduct were modeled on the ECPA and its predecessor the 1968 Act, some state court cases followed the *Simpson* holding in similar fact patterns. In the 1981 South Carolina case of *Baumrind v. Ewing*,[30] the wife in a matrimonial action sought to suppress certain recorded telephone conversations between herself and third parties made by her husband without her knowledge or consent. The court held that "the husband's conduct is beyond the grasp of [the 1968 Act]. Domestic conflicts are traditionally and properly

---

25 *Simpson*, 490 F.2d at 803.
26 *Id.* at 804.
27 *Id.* at 806.
28 *Id.*
29 *Id.* at 809.
30 279 S.E.2d 359.

matters of state interest."[31] Apparently, the *Baumrind* court was asserting – what the *Simpson* court might have been thinking but stopped short of saying – that Congress somehow lacks the authority to criminalize conduct between two persons who happen to be married.

The 1994 Mississippi case of *Stewart v. Stewart*[32] also involved the issue of whether an audio tape of a wife's conversation made by the husband violated the ECPA and should be allowed into evidence. The court held, following *Simpson* and the 1977 Second Circuit case of *Anonymous v. Anonymous*,[33] that since the husband and wife were married, and living in the same house, and both had access to the phones, the husband was within his rights to pick up an extension phone and listen to such conversation – and apparently therefore record it. "As such conduct is explicitly exempted from [the ECPA's] wiretapping prohibition, it can rationally be inferred that [the ECPA] does not prohibit a person from taping a conversation, within his own home, that he is legally authorized to listen to by picking up an extension phone."[34]

In 2003, the U.S. Court of Appeals for the Eleventh Circuit in *Glazner v. Glazner*[35] in a well-reasoned decision following time honored traditions of judicial review of statutes, affirmatively stated that the *Simpson* decision was wrong. *Glazner* held that there is no implied exception in the ECPA for interspousal wiretapping within the marital home.[36] Here the husband during a divorce proceeding placed a recording device on a telephone in the marital home and recorded conversations between his wife and a third party without either party's consent. The wife filed a complaint in the U.S. District Court for the Northern District of Alabama seeking damages under the ECPA. The district court, relying on the implied inter-spousal exemption from the *Simpson* line of cases, granted the husband's motion for summary judgement. On appeal, the Eleventh Circuit Court of Appeals examined the language of the ECPA and found it to be

---

31 *Id.* at 353.
32 645 So.2d 1319 (Miss. 1994).
33 558 F.2d 677 (2d Cir. 1977).
34 *Stewart*, 645 So. 2d at 1321.
35 347 F.3d 1212 (11th Cir 2003).
36 *Id.* at 1213.

unambiguous and stated the language of the statute made "no distinction between married and unmarried persons or between spouses and strangers. It plainly applies to 'any person' on both sides of the violation."[37] The court stated further that "the ECPA expressly gives 'any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of the [ECPA]' the right to bring a civil action against 'the person or entity . . . which engaged in that violation.'"[38] The court held that under the ECPA both husband and wife are "any person" and that the wife's conversations that her husband caused to be intercepted and recorded were indeed "any wire, oral, or electronic communication" within the plain language of the ECPA.[39] The *Glazner* court properly noted that "[a] court may only properly look beyond the plain language of a statute when giving effect to the language used by Congress would lead to a truly absurd result."[40]

Prior to *Glazner*, other federal courts had concluded that the court in *Simpson* improperly read an exception into the 1968 Act which simply was not there. The court in *Heyman v. Heyman*[41] found that the *Simpson* court's "search for congressional intent ignored the accepted canon of statutory construction that resort to legislative history is not ordinarily undertaken unless a statutory provision is unclear or ambiguous."[42]

Some of the strongest early criticism of *Simpson* came just five years after it was decided. In the 1979 case of *Krantz v. Krantz*[43] the husband hired a third party to install a tap on the family phone and recorded calls which disclosed his wife's extramarital affair. Upon discovery of the tap, the wife and her lover sued for damages under the 1968 Act. The husband argued that

---

37 *Id.* at 1215.

38 *Id.* at 1215, citing 18 U.S.C. § 2520(a).

39 *Id.* at 1215.

40 *Id.* at 1215, citing United States v. Maung, 267 F.3d 1113, 1121 (11th Cir. 2001), Merritt v. Dillard Paper Co., 120 F.3d 1181, 1188 (11th Cir. 1997).

41 548 F. Supp. 1041 (N.D. III. 1982).

42 *Id.* at 1045, citing United States v. Oregon, 366 U.S. 643, 648 (1961). By the general rules of statutory construction, legislative history is not ordinarily examined, since the best evidence of congressional intent is the text of the statute itself. Patagonia Corp. v. Board of Governors of Fed. Reserve Sys., 517 F.2d 803, 813 (9th Cir. 1975).

43 477 F. Supp. 463 (E.D. Pa. 1979).

interspousal wiretapping was not actionable under the statute. This argument was rejected by the court, which held that "the [1968 Act] means what it says, and prohibits all interceptions of wire communications, by any person, unless expressly provided."[44] The 1968 Act expressly states all of the exceptions that are provided for in such statute.[45] The legislative history of the 1968 Act is "not inconclusive, but evinces a congressional awareness of the widespread use of electronic eavesdropping in domestic cases, and a congressional intent to prohibit such eavesdropping."[46]

It does not appear that any reported case has followed the *Simpson* holding or reasoning after the *Glazner* case was decided in 2003 – making it clear that the provisions of the ECPA – both criminal and civil – should apply to conduct engaged in by a spouse in a matrimonial case or situation. Although federal criminal prosecutions for "spousal interceptions" under the ECPA are rare,[47] state criminal prosecutions for similar violations are more common,[48] as are federal civil cases seeking damages under the private right of action under the ECPA.[49]

A. *Statutory Civil Actions for Damages Arising from Violation of Criminal Statutes Prohibiting Interception of Electronic Communications*

18 U.S.C. Section 2520 provides that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter" may sue to recover civil damages.[50] Damages under this provision of the ECPA may include equitable or declaratory relief (injunction(s),

---

44 *Id.* at 467.

45 *Id.* at 468.

46 *Id.* at 470.

47 *See, e.g.,* United States v. Jones, 542 F.2d 661 (6th Cir. 1976).

48 *See, e.g.,* State v. Jock, 404 A.2d 518 (Del. Super. Ct. 1979); State v. Lombardo, 738 N.E.2d 653 (Ind. 2000); People v. Walker, No. 304593, 2011 WL 6786935 (Mich. Ct. App. Dec. 27, 2011); Williams v. Stoddard, C.A. No. PC 12-3664, 2015 WL 644200 (R.I. Super. Ct. Feb. 11, 2015); State v. King, 437 S.W. 3d 856 (Tenn. Crim. App. 2013); Duffy v. State, 33 S.W. 3d 17 (Tex. App. 2000).

49 *See, e.g.,* Kratz v. Kratz, 477 F. Supp. 463 (E.D. Pa. 1979); Heyman v. Heyman 548 F. Supp. 1041 (N.D. Ill. 1982); Resnik v. Coulson, 17-CV-676 (PKC) (SMG), 2020 WL 5802362 (E.D.N.Y. Sept. 28, 2020).

50 18 U.S.C. 2520 (a) (1986).

actual damages, statutory damages of $10,000 or $100 per day of violation, whichever is greater, punitive damages and reasonable attorneys fees and litigation costs.[51]

Several states have statutes modeled after 18 U.S.C. § 2520 or that closely follow the federal statute and provide a similar private civil right of action.[52] Other states, like New York and New Jersey, have statutes that criminalize the interception of electronic communications but do not provide any private civil right of action under the statute.[53]

Connecticut is one of the states that does provide for a private civil right of action for violation of its state's eavesdropping and wiretapping statute. Connecticut General Statute § 52-570(d) provides that "any person aggrieved by a violation of subsection (a) of this section may bring a civil action in the Superior Court to recover damages, together with costs and a reasonable attorney's fees"[54] The "subsection (a)" referred to is the provision of Connecticut General Statutes which prohibits the interception (and recording) of an oral private communication without the consent of all parties thereto.[55]

The District of Columbia also provides for a private right of action for violations of its 'wiretapping' statute following almost verbatim the ECPA.[56]

In 2016 the U.S. Court of Appeals for the Seventh Circuit in *Epstein v. Epstein*[57] held that a husband had the right to bring a civil action against his wife pursuant to 18 U.S.C. § 2520 where the wife had intercepted his emails in violation of the ECPA. In

---

51 18 U.S.C. 2520 (b), (c) (1986).

52 *E.g.,* FLA. STAT. § 934.27 (2019); 720 ILL. COMP. STAT. § 5/14-6; MASS, GEN. LAWS ch 272 § S99 (2019); MICH. COMP. LAWS § 750.539h (2019); 18 PA. CONS. STAT. § 5747 (2019); TEX. CIV. PRAC. & REM. CODE § 123.002 (2019).

53 *See* N.Y. PENAL LAW art. 250; N.J. STAT. ANN. 2A:156-24*, et seq.*

54 CONN. GEN STAT § 52-570d (2019).

55 CONN. GEN STAT § 52-570(a) (2019). Note: unlike New York and other "one party" states which permit interception when one party to the communication has consented, consistent with federal law, Connecticut and a handful of other states (California, Florida, Hawaii, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania, and Washington) require the consent of all parties for an interception or recording of electronic communication to be lawful).

56 D.C. CODE § 23–554.

57 843 F.3d 1147 (7th Cir. 2016).

Epstein, the wife surreptitiously placed an auto-forwarding "rule" on husband's email accounts that automatically forwarded the email messages to herself.[58] The ECPA makes it unlawful to "intentionally intercept [or] endeavor . . . to intercept . . . any wire, oral, or electronic communication."[59] The ECPA also prohibits the intentional "Disclos[ure] or use . . . of the contents of an unlawfully intercepted electronic communication."[60] "[I]ntercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication."[61] "[E]lectronic communication," is "any transfer of signs . . . of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system."[62]

The parties argued in great detail about whether or not the ECPA requires a "contemporaneous interception" of an electronic communication, in other words, "an interception that occurs during the transmission rather than after the electronic message has come to rest on a computer system."[63] The court found that there was in fact a contemporaneous interception of an electronic communication based on the "auto forwarding" of the emails.[64] Here the court found that the "interception of an email need not occur at the time the wrongdoer receives the email; . . . [t]he copying at the server was the unlawful interception."[65]

The distinction drawn by the court regarding the contemporaneous nature of the interception based on the email forwarding is important – since many factual situations that presented in these types of cases involve interception through similar means – whether through email forwarding rule, spyware interception programs, or services being exploited to "auto forward" copies of

---

58 *Id.* at 1149.

59 18 U.S.C. § 2511(1)(a).

60 *Id.* at § 2511(1)(c), (d).

61 *Id.* at § 2510(4).

62 *Id.* at § 2510(12).

63 *Epstein*, 843 F.3d at 1149, citing United States v. Szymuszkiewicz, 622 F.3d 701, 703 (7th Cir. 2010). Several circuits have held that the Wiretap Act covers only contemporaneous interceptions—understood as the act of acquiring an electronic communication in transit.

64 *Id.* at 1151.

65 *Id.* at 1150, citing *Szymuszkiewicz*, 622 F.3d at 704.

text messages.[66] These all represent unlawful interceptions under the ECPA.

In 2012, the U.S. District Court for the Eastern District of Tennessee in the matter of *Klumb v. Goan*[67] found that a wife had violated the ECPA and the Tennessee Wiretap Act[68] by installing spyware on her husband's computers without his consent to intercept his incoming email in connection with an ongoing matrimonial action. Tennessee Code § 39-13-603 (the "TWA") is Tennessee's counterpart to 18 U.S.C. § 2520. It states in relevant part: "any aggrieved person whose wire, oral or electronic communication is intentionally intercepted, disclosed, or used in violation of § 39-13-601 . . . may in a civil action recover from the person or entity that engaged in that violation."[69] The court awarded the plaintiff statutory, liquidated damages of $10,000 for each violation of the ECPA and the TWA, punitive damages of $10,000, and reasonable attorney's fees and expenses.[70]

There is nothing in the language of the ECPA that would make a criminal prosecution or conviction under the Act a condition precedent to maintaining or prevailing in a civil suit for damages under the private right of action provided in the statute and there does not appear any to be any reported case holding that a prior conviction is required. On the contrary, it appears that most civil cases brought under the Act and corollary state statutes are brought in the absence of any such criminal proceeding(s).[71]

As is clear from the statutes and cases discussed above, the use of any mechanism or method to intercept the emails, text messages or other electronic communications of one's spouse is a criminal offense in every state and territory of the United States, and gives rise to statutorily authorized civil damages. The dissemination or use of such intercepted communications is also a criminal offense, and there is civil liability by statute not only against

---

66 See *infra* discussion in text at notes 72-73.

67 884 F. Supp. 2d 644 (E.D. Tenn. 2012).

68 TENN. CODE ANN. § 39-13-601.

69 *Klumb*, 884 F. Supp. 2d at 660.

70 *Id.* at 665-67.

71 Resnick v. Coulson, 1:17-cv-00676-PKC-SMG (E.D.N.Y. Mar. 30, 2019). *See, e.g., Klumb*, 884 F. Supp. 2d 644; *Epstein*, 843 F.3d 1147; *Glazner*, 347 F.3d 1212.

the "interceptor" but also against any person who disseminates or uses such material with knowledge of its source under federal law, and many concomitant state statues.

As serious as these consequences may seem, however, they are apparently insufficient to deter what this author has observed to be a steady increase in this prohibited conduct by all manner of ingenious (and not so ingenious) methods. In one recent case, the estranged husband, who was living outside the marital residence during the divorce proceedings, visited with his children at the marital home. While the husband was taking a dip in the pool with the kids, the wife took his smartphone from the kitchen counter where he had laid it down and before it could auto lock she used the browser on the phone to visit the cell carrier's website and sign up for a service known as Verizon Messaging Plus. The carrier sent several confirmation texts to the husband's phone, which the wife promptly deleted. The wife did not "install" anything on the phone, merely activated a service provided by the carrier at the network level. This service allowed her to input an alternate cell number to which the carrier would contemporaneously send copies of all the husband's incoming and outgoing text messages. Using this service, the wife continued to receive all of the husband's text messages for six months before a forensic examination of the husband's phone discovered the deleted text messages showing the phone was subscribed to this service (and when). Over the past several years, the author has seen cases like this at the rate of at least one per week. Clearly, our technology has exceeded our humanity.

B. *Prohibition on Use of Intercepted Communications as Evidence*

If the criminal and civil penalties for unlawful interception are not enough to dissuade would be spousal interceptors, there are still other, independent reasons why engaging in this conduct is simply not worth the risks.

Although many states continue to follow the common law rule that illegally obtained evidence may be admissible if it is relevant and material, this common law rule applies only in the absence of some statutory or constitutional provision to the

contrary.[72] Many states do in fact have statutory provisions that specifically prohibit unlawfully intercepted electronic communications from being used as evidence.[73] While federal law mandates the exclusion of intercepted "wire or oral communications" from evidence in any federal or state court proceedings,[74] this exclusionary provision does not extend to intercepted "electronic communications" (such as emails or text messages).[75] The reasons for this are unclear, but the language of the statute is not.

There are, to be sure, a number of state court decisions holding that intercepted electronic communications may be admissible in a matrimonial case despite the potential criminality of the conduct in obtaining them. In the 1974 case of *Beaber v. Beaber*,[76] the Court of Common Pleas in Stark County, Ohio, held that neither the Ohio statutes, the Ohio Constitution, nor the federal Constitution as it related to the right of privacy, prevented the admission of evidence obtained in violation of Ohio's eavesdropping and wiretapping statutes in a matrimonial action. Prior to the commencement of the matrimonial action in that case, the husband had tapped his home phone and recorded conversations between his wife and a third party. Based on those recordings and other factors, the husband commenced a matrimonial action and sought to bring the tapes into evidence.

The court considered various Ohio statutes regarding eavesdropping and wiretapping along with the 1968 Act as the predecessor to the ECPA. The court found no Ohio cases directly on point, and ironically enough cited *Sackler v. Sackler*,[77] a 1964 case from New York State's highest court, decided before the 1968 Act was enacted, which held that just because evidence was obtained illegally did not destroy its credibility or admissibility

---

72 *See, e.g.*, Sackler v. Sackler, 15 N.Y.2d 40 (1964); Stagg v. NYC Health & Hosp. Corp. 162 A.D.2d 595 (N.Y. App. Div. 1990).

73 *See, e.g.*, CONN. GEN. STAT. §§ 54-41a – 54-41t (Connecticut Wiretap Statutes); KAN. STAT. ANN. § 22-2517 (Kansas Wiretap Act); MD. CODE ANN. CTS. & JUD. PROC. § 10-402 (Maryland Wiretap Act); N.Y. C.P.L.R. § 4506; 18 PA. CONS. STAT. ANN. § 5721 (Pennsylvania Wiretap and Electronic Surveillance Act).

74 18 U.S.C. § 2515.

75 *See* United States v. Steiger, 318 F.3d 1039, 1050-52 (11th Cir. 2003); United States v. Jones, 364 F. Supp. 2d 1303, 1308-09 (D. Utah 2005).

76 322 N.E. 2d 910 (Ohio Com. Pleas 1974).

77 15 N.Y. 2d 40, 203 N.E. 2d 481, 255 N.Y.S.2d 83 (1964).

provided it was otherwise relevant and material.[78] What the *Beaber* court failed to mention, however, is that while *Sackler* did arise out of a matrimonial action, and did involve the question of whether to suppress unlawfully obtained evidence, the evidence sought to be suppressed in *Sackler* (and was ultimately ruled admissible by the New York Court of Appeals), was evidence obtained by means of an illegal forcible entry into the wife's home by the husband and private investigators - *not illegally intercepted electronic communications*.[79] In ruling that the evidence in question was not inadmissible merely because of the manner in which it was obtained, the Court of Appeals in *Sackler* made reference to New York statutes, stating "the New York Legislature, when it has found necessity for outlawing evidence because it was secured by particular unlawful means, has provided specific statutory prohibitions *such as those against the use of proof gotten by illegal eavesdropping*.[80]

The *Beaber* court stated, "neither the Fourth Amendment to the U.S. Constitution nor the prohibition against unreasonable search and seizures in the federal and state constitutions applied to acts by nongovernmental persons — in this case the defendant — and such provisions do not apply in civil cases."[81] The court also cited *Simpson v. Simpson*, and held that "neither the statutes, the Ohio Constitution, the federal Constitution as it related to the right of privacy, nor the Act prevent the admission of said tapes."[82]

While Ohio would appear to allow unlawfully intercepted electronic communications into evidence in a matrimonial action, many other states, including Connecticut, Kansas, Maryland, New York, and Pennsylvania, would not.[83] So even if a party were willing to risk the serious criminal and civil liabilities for violating the ECPA and similar state statutes prohibiting inter-

---

78 *Id.* at 44

79 *Id.* at 42.

80 *Id.* at 44, citing N.Y. C.P.L.R. § 4506.

81 *Beaber*, 322 N.E.2d at 914 (emphasis added).

82 *Id.* at 104.

83 *See* Conn. Gen. Stat. §§ 54-41a – 54-41t (Connecticut Wiretap Statutes); Kan. Stat. Ann. § 22-2517 (Kansas Wiretap Act); Md. Code Ann. Cts. & Jud. Proc. § 10-402 (Maryland Wiretap Act); N.Y. C.P.L.R. § 4506; 18 Pa. Cons. Stat. Ann. § 5721 (Pennsylvania Wiretap and Electronic Surveillance Act).

ception of electronic communications, in many jurisdictions they would be prohibited from using the fruits of their unlawful endeavors as evidence in their matrimonial case.

III. Direct Sanctions in Matrimonial Court for Interception of Electronic Communications

For many years it seemed matrimonial courts did not wish to get sidetracked delving into the alleged misdeeds of parties before them when those allegations consisted of unlawful recording or interception of electronic communications. Perhaps the sentiment was that parties aggrieved by such conduct had remedies elsewhere: they could file a criminal complaint or civil action for money damages and/or injunctive relief outside of the matrimonial litigation. That sentiment, if it existed, seems to be waning. Recent matrimonial cases have tended to pay more attention to these allegations (especially when the alleged interception involved privileged communications) and have imposed direct and substantial sanctions in the matrimonial case against the party who violated the ECPA and/or similar state statutes. In at least one such case, the court went so far as to strike the guilty party's pleadings upon a finding that the party had unlawfully intercepted the opposing party's communications, including privileged communications, and had engaged in spoilation of evidence regarding that conduct.

In the 2018 case of *CC v. AR*[84] the New York Supreme Court in Kings County, upon a finding that the plaintiff husband (the non-monied spouse in that case) had, among other things, installed spyware on his wife's iPhone to track her movements using GPS, and intercept her emails, texts, and phone conversations, determined the appropriate sanction was to strike the plaintiff husband's pleadings related to all claims for financial relief (except for the issue of possible child support should he be awarded custody).[85] The foundation for the court's decision in that case was extensive discovery and detailed reports of the court appointed attorney referee, supported by voluminous reports of computer forensic professionals confirming that the husband had installed the spyware in question on the wife's iPhone

---

84 100 N.Y.S.3d 609 (N.Y. Sup. Ct. 2018).

85 *Id.* at 639.

and had intercepted her electronic communications through that method. Evidence was also presented that the husband engaged in the use of wiping programs to permanently erase data from his own computing devices – which the court presumed was further evidence of the husband's misconduct in this regard.[86] In the decision, Judge Sunshine wrote:

> Under the unique facts and circumstances of this case, a lesser spoliation sanction—including issue preclusion—would neither address the gravity of the plaintiff's contemptuous behavior nor restore defendant to an ability to participate on equal footing with the plaintiff given plaintiff's egregious conduct both of months of surreptitious spyware monitoring of defendant's attorney-client privileged communications and meetings and his intentional and bad faith destruction of the key evidence when he learned that his computing devices were going to be seized.[87]

The court in *CC v. AR* was, as far as this author can determine, the first matrimonial court to actually strike a party's pleadings based on these facts.

IV. Distinguishing Unlawful Interception from Lawful Collection and Preservation of "Static ESI" from Computing Devices in the Marital Residence (or Domain) – a/k/a "Clandestine Imaging"

While the interception of electronic communications through virtually any means is a criminal offense absent consent, and gives rise to civil liability under the federal and many state statutes, and the evidence thus obtained is often deemed inadmissible, the collection and preservation of "static ESI" from a computing device or devices within the marital residence (referred to by this author as "clandestine imaging"[88]) is in certain

---

86 *Id.*

87 *Id.*

88 "Imaging" is a term of art, referring to a method of copying data from a computing device in a forensically sound manner, which involves the creation of a bit for bit copy of the data which can be verified and authenticated at all future times through a process known as "hashing."

cases legal and appropriate, and the evidence obtained may be perfectly admissible.[89]

The benefits of clandestine imaging are undeniable. Because the opposing party does not know that the information is being gathered, that party does not have an opportunity to manipulate or destroy it, and cannot "lose" the entire computing device or conveniently have it suffer a fatal crash prior to its discovery and inspection through formal discovery mechanisms. In short, the opposition does not have an opportunity to engage in spoilation through wiping as occurred in the case of *CC v. AR*, discussed above.[90]

Clandestine imaging can be extremely useful, even when no immediate analysis of the acquired data is contemplated or pursued. Simply securing a forensic image of the hard drive of a family computer in the marital residence gives the litigant who collects that data an "ace in the hole." That party now possesses a forensically perfect duplicate of all data on that device, "frozen in time," before the other spouse has notice of the litigation or a motion to compel production of the device(s) for discovery and inspection. This "ace in the hole" can be used to keep the other side honest, for example by using it to randomly audit the completeness and accuracy of financial discovery provided by the other spouse. Take the example of a laptop computer in the marital home, primarily used by the monied spouse, but occasionally utilized by the non-monied spouse. The non-monied spouse has the hard drive of that laptop computer forensically imaged prior to the commencement of the litigation. The data is secured, but not analyzed. The case then begins, and discovery ensues. The monied spouse provides information requested in discovery, but the non-monied spouse and/or their counsel suspects that the information produced in discovery is incomplete or not authentic. An examination of the acquired hard drive image can proceed at that point to determine if responsive information exists that was not produced, or if the information produced was altered or manipulated in any way. Another strategy is for counsel representing the spouse who has engaged in the clandestine imaging to

---

89 *See, e.g.,* Byrne v. Byrne, 650 N.Y.S.2d 499 (N.Y. Sup. Ct. 1996); Moore v. Moore, N.Y.L.J. (N.Y. Sup. Ct. 2008); Gurevich v. Gurevich, 24 Misc. 3d 808 (N.Y. Sup. Ct. 2009).

90 *See supra* discussion in text at notes 81-82.

notify the other side after commencement of the case, that his/her/their client has a forensic image of the computing device in question as of a specific date. Such "notice" will obviously tend to dissuade the opposing party from any effort to destroy, manipulate, or otherwise make discoverable data "unavailable."

Given the benefits of clandestine imaging, it is important to examine the legality of this conduct. Case law in a number of states is directly on point, and clearly indicates that under certain circumstances, this type of self-help – *which does not involve the contemporaneous interception of any electronic communications* – is legal, and the resulting evidence should be admissible.

Three New York cases on point are particularly illustrative on the issue of the legality and admissibility of data retrieved from a computer in a matrimonial situation without the knowledge of the other party. Pertinent state statutes must also be considered since they may be directly controlling on these issues and vary from state to state. The relevant New York statutes are discussed below.

The seminal New York decision on this issue is *Byrne v. Byrne*[91] decided in 1996. Despite its age, *Byrne* remains good law and has been cited numerous times for the proposition that a computer in the marital residence is the equivalent of a filing cabinet. Each spouse has access to the computer in much the same way either could physically open a filing cabinet. In *Byrne*, the court arrived at this decision even though the computer was admittedly the property of the husband's employer and not actually owned by either spouse. The decision hinged on the computer's presence in the home and its physical availability to both spouses.

The real issue is not who possesses the computer but rather who has access to the computer's memory. The computer memory is akin to a file cabinet. Clearly, a plaintiff could have access to the contents of a file cabinet left in the marital residence. In the same fashion she should have access to the contents of the computer. The plaintiff seeks access to the computer memory on the grounds that defendant stored information concerning his finances and personal business records in it. Such material is obviously subject to discovery. Therefore, it is determined that the

---

91 650 N.Y.S.2d 499 (N.Y. Sup. Ct. 1996)

plaintiff did nothing wrong by obtaining the physical custody of the notebook computer.[92]

The 2008 case of *Moore v. Moore*[93] involved a laptop computer that a wife had taken from her husband's car. This laptop was turned over to the wife's counsel and the attorneys for both spouses stipulated that the husband's password would be provided, and that discovery would be permitted from the computer. Apparently having second thoughts, the husband sought to suppress the contents of the laptop pursuant to New York Civil Practice Law and Rules § 4506, claiming that the wife had violated Article 250 of the New York Penal Law, discussed above, which makes it a Class E felony to intercept an electronic communication without the consent of at least one party.

The court disagreed with the husband and ruled that there was no eavesdropping offense, no penal law violation and no need to suppress anything from the computer's hard drive.[94] The court stated that the hard drive's record of *past communications* is not susceptible to "interception" under the statute. This analysis is key to understanding why this type of self-help in the context of spouse versus spouse in a matrimonial action is in most cases perfectly legal, as opposed to the deployment or use of spyware or other methods that actually intercept emails, instant messages or other electronic communications in real time.

The case of *Gurevich v. Gurevich*[95] presents a slightly different set of circumstances, and is the case that is most often referred to by those who would argue clandestine imaging in the marital context is potentially a violation of the criminal law. A careful analysis of this case, and the statutes referenced and discussed in the decision is required. In *Gurevich*, the wife, a software developer, had used the husband's password to access the husband's email account and obtain his emails after the divorce action commenced. The husband's attorney attempted to exclude from evidence the emails obtained by the wife, citing New York New York Civil Practice Law and Rules § 4506, discussed above, which makes evidence obtained in violation of New York Penal Law Article 250 inadmissible in any civil pro-

---

92 *Id*. at 499.

93 N.Y.L.J. 26 (N.Y. Sup. Ct. Aug. 14, 2008).

94 *Id.* at 26, col 1.

95 24 Misc. 3d 808 (N.Y. Sup. Ct., Kings Co. May 5, 2009).

ceeding in New York. The court held that there was no eavesdropping violation under Penal Law § 250 (citing *Moore*).[96] In this case the court reviewed the legislative history of New York Penal Law § 250.05 for guidance. In doing so, the court determined from a reading of the statute, legislative history, and case law that the purpose of Penal Law § 250.00 is to prohibit individuals from intercepting communications going from one person to another. The court found that the e-mail was not "in transit" but stored in the e-mail account, and accordingly failed to fall within the scope of § 4506.[97] This should have ended the inquiry, however, the court went on to state, in dicta, that there may have been a violation of the computer tampering/computer trespass statues under New York Penal Law Article 156[98] without providing any further analysis or reasoning for that statement. The court said it did not need to reach a conclusion on this issue because suppression under § 4506 applies only to evidence obtained in violation of Penal Law Article 250, which the court already concluded had not been violated.

Admissibility of evidence issues aside, the court's reference in *Gurevich* to a possible violation of New York Penal Law § 156.10 (Computer Trespass, a Class E Felony) is certainly serious enough to warrant concern, at least until the issue is thoroughly analyzed. While the court in *Gurevich* did not discuss (understandably, because it was not adjudicating a criminal matter) when suggesting that the collection of the evidence by the wife in this case "might" be a violation of New York Penal Law §§ 156.05 and 156.10 (Unauthorized Use of Computer, Computer Tampering, Computer Trespass) is that Article 156 of the New York Penal Law contains an express defense to any charge under that article. Such express defense is that if "the defendant had reasonable grounds to believe that he had authorization to use the computer" or "had reasonable grounds to believe that he had

---

96 *Moore*, N.Y.L.J., at 26, col 1. There the court held that Penal Law § 250.05 did not apply to the facts presented because in accessing the disputed files, the plaintiff did not intercept, overhear, or access electronic communications. The communication was saved to the hard drive by the husband, and the wife's subsequent access to that material downloaded and saved to the hard drive of the computer was not the result of an intercepted communication and did not constitute a violation of Penal Law § 250.05.

97 *Gurevich*, 24 Misc. 3d at 811.

98 *Id.* at 813.

the right to copy, reproduce or duplicate in any manner the computer data or the computer program."[99]

In light of *Byrne v. Byrne*,[100] *Moore v. Moore*,[101] and similar cases it is difficult to imagine a persuasive argument that a spouse would not have "reasonable grounds to believe" that they had authorization to access a computer in the marital residence, or copy, reproduce, or duplicate data on that computer in the context of seeking potential evidence relevant to a matrimonial litigation. In addition, under the New York Penal Law, a defense such as the defense to Article 156 described above, is distinguished from an "affirmative defense" in that a defense need merely be raised by a defendant and must thereafter be *disproved beyond a reasonable doubt* by a prosecutor whereas an "affirmative defense" must be pleaded and proved by the defendant.[102] Given this framework, it is nearly impossible to imagine a prosecutor bringing a criminal case against a spouse who merely copies data from a computing device in the marital residence (or as seemingly expanded by the court in *Moore* to the "marital domain" since the laptop in question in that case was removed by the wife from the husband's car) as opposed to "intercepting" their spouse's electronic communications, which is without question a criminal offense under federal law and the laws of most states absent consent.

Conclusion

When "digital spousal espionage" includes the interception of electronic communications, it can result in extremely serious consequences including criminal charges, civil suits for statutory damages and attorneys' fees, extreme sanctions against the guilty party in a matrimonial litigation (up to and including the striking of pleadings), not to mention the likelihood of the 'evidence' gathered being ruled inadmissible. Covert collection (*i.e. clandestine copying – not intercepting*) of data from a computing device in the marital residence however, may be perfectly permissible in many jurisdictions (and is certainly not unlawful

---

99 N.Y. Penal Law §156.50 (1), (2) and (3).

100 168 Misc. 2d 321, 650 N.Y.S. 2d 499 (N.Y. Sup. Ct. 1996).

101 N.Y.L.J. (N.Y. Sup. Ct. Aug. 14, 2008).

102 *See* N.Y. Penal Law § 25 Defenses; Burden of Proof.

under federal law), but the interception of electronic communications through virtually any means, without consent, is almost certain to be a violation of law. The spectrum of extremely serious consequences notwithstanding, this author has witnessed (and reported cases and media stories in recent years corroborate) a sharp rise in cases involving the unlawful interception of electronic communications in matrimonial (and other domestic relations) cases. There are only two rational conclusions that can be drawn from these facts: either matrimonial litigants do not know what they are doing is illegal and can have potentially severe consequences, or they simply do not care and are willing to take the risk. This author has been witness to cases where the latter is true. The author believes however, that in the vast majority of cases, it is the former, and the "guilty" party did not know that their conduct was "illegal" – or more precisely, they had no idea 'just how illegal it was!'. If this is true, then matrimonial attorneys would be doing their clients a tremendous service by counselling them early on in the representation, and without waiting for the issue to come up, what 'interception of electronic communications' entails, how it occurs, how it is different from 'copying' data from a computing device in the marital home, and just how serious the consequences of unlawful interception can be. In addition to helping an "ignorant" client who might be contemplating such conduct to avoid the potentially serious consequences of same, counsel will also be alerting clients who have no intention of engaging in such conduct, that this type of conduct not only occurs, but how prevalent it has become through such a wide variety of methods, and to be on the lookout for any indication that they may be a victim of same. If there are indications that unlawful interception may have occurred, given the potential remedies available, counsel would be wise to enlist the assistance of computer forensic professionals to collect and preserve the evidence of same.