At an IAS Part 5G of the Supreme Court of the State of New York, held in and for the County of Kings, at the Courthouse, at Civic Center, Brooklyn, New York, on the 5th day of February, 2018.

P R E S E N T:

HON. JEFFREY S. SUNSHINE,
Justice.

- -x

CROCKER C.,

Plaintiff,

- against -

ANNE R.,

Defendant.

- -x

Index No.: REDACTED

DECISION & ORDER
Motion Seq. #25

The following papers numbered 1 to 4 read herein:

	Papers Numbered
Notice of Motion/Order to Show Cause/ Petition/Cross Motion and Affidavits (Affirmations) Annexed	1,
Opposing Affidavits (Affirmations)	2,
Reply Affidavits (Affirmations)	3,
Other ___Attorney for the Children affirmation dated July 17, 2017	4

Crocker C. *Plaintiff Pro Se*	Raoul Felder and Partners By: Raoul Felder *Attorney for Defendant* 437 Madison Avenue New York, New York 10022	Louisa Floyd, Esq *Attorney for the Children* 26 Court Street, Suite 1917 Brooklyn, New York 11242

Introduction and Background

What remedies are available to an innocent spouse and her counsel when a marriage gets "hacked" and what remedies are available to the Court when the "hacking"

included intercepting the innocent spouse's attorney-client privileged communications and the "hacking" spouse then purposefully engaged in spoliation of the evidence while simultaneously asserting his Fifth Amendment right against self-incrimination?

In the instant matter the plaintiff-husband continues to assert his Fifth Amendment right against self-incrimination when questions as to whether he installed and used sophisticated spyware on the defendant-wife's iPhone to monitor all of her communications – and to access her attorney-client privileged communications – and also used that spyware to activate the microphone on the defendant's iPhone to "listen in" on her ambient conversations, including her attorney-client meetings, her sessions with her psychiatrist and conversations between her and her friends and family for more than four (4) months. Plaintiff further asserted his Fifth Amendment right against self-incrimination related to questions about his attempts to "data wipe" the evidence of his actions from his computing devices when he learned that the Sheriff of the City of New York had been ordered by the Court, after an *ex parte* emergency application by the defendant, to seize his computing devices. What is the role of the Court to protect the integrity of the process when a plaintiff in a civil action refuses to answer any questions related to his spyware usage – asserting his Fifth Amendment right against self-incrimination – while continuing to seek affirmative relief after having apparently engaged in extensive, intentional and bad faith spoliation of the key evidence?

On July 11, 2017, defendant-wife, moved by emergency order to show cause [motion sequence # 25] requesting the following relief: "1) holding the plaintiff in contempt for his patent violations of at least two prior Orders of this Court by virtue of his clear and unequivocal spoliation and destruction of evidence; 2) precluding the plaintiff from introducing at trial any evidence or testimony with respect to the issues of custody, access, equitable distribution, maintenance and/or child support, counsel fees, expert fees, Judge Belen's fees, etc.; and 3) granting defendant such other and further relief as this Court may deem just and proper."

Plaintiff-husband, *pro se*, filed an affidavit in opposition dated July 17, 2017. Plaintiff has discharged two (2) attorneys during the course of this litigation who had, in part, been paid substantial fees by the defendant-wife herein. Defendant-wife's counsel filed a reply affirmation dated July 20, 2017. The attorney for the children filed an affirmation in response dated July 17, 2017. The Court heard oral argument on the motion on September 8, 2017. At oral argument plaintiff, *pro se*, declined to orally argue despite the opportunity to do so and stated on the record that he chose to rely on his papers and waived his right to provide oral argument. Defendant's counsel and the attorney for the children participated in oral argument.

Procedural History

Plaintiff, through former counsel, commenced this action for divorce on October

28, 2014. Defendant appeared with counsel. The parties have engaged in extensive and complex motion practice during this litigation with both parties raising counter-accusations regarding the other parties' fitness and ability to parent their two (2) young children, twins, who are currently eight (8) years of age. The plaintiff-husband is fifty-three (53) years old and a freelance investor relations consultant.[1] The plaintiff has a BA from Yale University and was a Fulbright Scholar. The defendant-wife is fifty-three (53) years old and a freelance copy editor.[2] The defendant has a BA from Connecticut College and a MA in Education from Columbia University. The parties were married in June 2008.

The issue of spyware was first raised by defendant's counsel by *ex parte* application to the Court on Friday, May 15, 2015. An affidavit from defendant's computer expert based on an examination of defendant's iPhone detailed that spyware had been installed on that device as early as October 6, 2014. Defendant's counsel averred in his affirmation in support of that application that he had exchanged more than two hundred (200) e-mail communications protected by attorney-client privilege with the defendant between October 2014 and February 6, 2015 when defendant hired a computer expert who discovered the spyware on her iPhone. Defendant's counsel argued that if plaintiff was using the spyware he installed on defendant's iPhone that he had access to

[1]Plaintiff's occupation as listed on his affidavit of net worth dated December 3, 2014.
[2]Plaintiff argues in the May 28, 2015 affidavit that "defendant's money is derived mostly

those attorney-client privileged communications. He argued that if plaintiff accessed those attorney-client privileged electronic communications then he had prejudiced defendant's ability to participate in the litigation on a level playing field rather than a playing field where plaintiff had surreptitiously gained "insider" knowledge of defendant's litigation strategy. Defendant's counsel alleged that data uncovered by defendant's computer expert from an examination of defendant's iPhone revealed that, while the parties were living together during the marriage and approximately three (3) weeks before plaintiff commenced this matrimonial action, plaintiff breached defendant's iPhone security and installed spyware (mSpy). Defendant's counsel asserted that the spyware installed was tantamount to "bugging" defendant's iPhone. Defendant's counsel argued that the spyware gave plaintiff the ability to access in real-time "all of Defendant's communications, including her privileged communications, such as her e-mails, text messages, call history and logs, as well as other information, including the ability to access the Defendant's physical location via GPS tracking." He further argued that plaintiff "bugged" defendant's iPhone without her knowledge or consent and then used his access to surreptitiously and remotely intercept, access and monitor her communications from his computing devices. He further alleged that plaintiff covered up his access of defendant's communications by attempting to conceal his internet identity using a software program called IPVANISH.

---

from her late-father's roles as CEO and Chairman of [a major tobacco company]."

Defendant's counsel alleged that plaintiff's bank records and credit card statements produced during discovery related to the matrimonial action "reveal that he purchased, several times, the mSpy spyware program as well as the IPVANISH program..." Defendant's counsel affirmed that when he questioned plaintiff during his deposition on May 5, 2015 about these purchases and whether he installed spyware on defendant's iPhone the plaintiff laughed and invoked his Fifth Amendment privilege against self-incrimination approximately fifty-eight (58) times. He argued that the spyware on defendant's iPhone together with plaintiff's financial records showing the purchase of the spyware and plaintiff's consistent assertion of his Fifth Amendment privilege in response to all deposition questions related to the purchase or use of spyware were the basis for the emergency application.

Defendant's counsel filed an affirmation of emergency pursuant to 22 NYCRR 202.7(f) affirming that he did not notify plaintiff or plaintiff's counsel regarding the application and relief requested because "[g]iving them notice will result in significant prejudice to the Defendant in that the Plaintiff will have an opportunity – all it will take is for the Plaintiff to click one button or find one dumpster – to alter or destroy [*emphasis in original*]" evidence of his alleged "illegal wiretapping" of defendant and any interception of her confidential and privileged communications.

This Court issued the following order in response to the *ex parte* application[3]:

> ORDERED: Defendant's counsel shall service of copy of this Order to Show Cause upon the Sheriff of the City Of New York at SHERIFF'S HEADQUARTERS, EVIDENCE ROOM, 3010 STARR AVENUE, LONG ISLAND CITY, NEW YORK 11101 no later than Monday, May 18, 2015 at 10:00 a.m.; and it is further,
>
> ORDERED: That the Sheriff of the City Of New York shall personally serve this Order to Show Cause and supporting affidavits and affirmations to plaintiff no sooner than Monday, May 18, 2015 at 1:00 p.m.; and it is further,
>
> ORDERED: That the Sheriff of the City Of New York shall facsimile an affidavit of service to defendant's counsel (TELEPHONE NUMBER OMITTED) and to the Court (TELEPHONE NUMBER OMITTED) forthwith when service of this Order to Show Cause has been made upon plaintiff; and it is further,
>
> ORDERED: That upon notice from the Sheriff of the City Of New York that service upon plaintiff is complete the defendant's counsel shall forthwith personally serve to plaintiff's counsel the Order to Show Cause, together with supporting documents; and it is further,
>
> ORDERED: Upon presentation of this order, plaintiff shall immediately turn over to the Sheriff of the City Of New York for safekeeping, under seal, any and all computing devices, including without limitation, any personal or business computer, external hard-drives, iPad, cellular telephone and/or devices having networking/internet capability in his possession; and it is further,

[3]Defendant's emergency application was made on the afternoon of Friday, May 15, 2015. To ensure that plaintiff was without his computing devices for the shortest duration of time before he could be heard on defendant's application, while also providing plaintiff an opportunity to confer with his counsel after service of the order to show cause and prior to the return date, the Court directed that the Sheriff of the City Of New York seize and hold any computing devices received from plaintiff in connection with the Friday, May 15, 2015 order after 1:00 P.M. on Monday, May 18, 2015. The Court set the return date of defendant's order to show cause for Wednesday, May 20, 2015 at 9:30 A.M. In doing so, the Court crafted relief intended to safe-guard plaintiff's due process rights and to avoided a situation where plaintiff was deprived of his computing devices for the upcoming weekend.

ORDERED: That the Sheriff of the City Of New York is directed to take and to hold any devices received from plaintiff in connection with this order until further order of the Court; and it is further,

ORDERED: The plaintiff shall not, until further order of the Court, delete, sanitize or alter any information stored in online storage accounts, "clouds" or any other accounts that store digital information; and it is further,

ORDERED: The plaintiff shall not, until further order of the Court, authorize or direct any other individual to delete, sanitize or alter any information stored in online storage accounts, "clouds" or any other accounts that store digital information; and it is further,

ORDERED: The plaintiff shall not, until further order of the Court, access or authorize or direct any other individual to access any accounts with mSpy, Pangu, IPVANISH, and/or any other related or similar entity or affiliate or related software or program; and it is further,

ORDERED: The plaintiff is, until further order of the Court, restrained and enjoined from destroying, tampering with or disposing of the originals and/or copies of any and all records, in any form, related to purchase and/or use of services from mSpy, Pangu, IPVANISH, and/or any other related or similar entity or affiliate or related software or program and he shall not authorize or direct anyone else to destroy, tamper with or dispose of the originals and/or copies of any and all records, in any form, related to purchase and/or use of services from mSpy, Pangu, IPVANISH, and/or any other related or similar entity or affiliate or related software or program; and it is further,

ORDERED: That neither the Sheriff of the City Of New York, the Sheriff of the City Of New York's representatives, the defendant or defendant's attorneys or agents shall have access to the contents on any said devices pending further order of the court; and it is further,

ORDERED: The part clerk of Part 5G shall maintain original order to show cause under seal in the above-captioned file until such time as service has been accomplished or pending further order of the Court and no further entry shall be made on the Court's computer system shall be made pending

> notice of service having been accomplished as detailed herein by the Sheriff of the City of New York; and it is further, ...

The May 15, 2015 *ex parte* order also provided, as relevant hereto,

> ORDERED: The Sheriff of the City Of New York is directed to serve a copy of the continued temporary order of protection on plaintiff no sooner than Monday, May 18, 2015 at 1:00 p.m. together with the Order to Show Cause and supporting papers as detailed herein above; and it is further,
>
> ORDERED: The minutes of today's proceeding are sealed until such time as service is accomplished by the Sheriff of the City of New York or further order of the Court.

On May 20, 2015, plaintiff and his then counsel appeared and requested time to submit opposition papers to defendant's emergency order to show cause. Defendant's counsel, on the record, argued that he believed plaintiff had engaged in tampering or deleting evidence remotely through the "Cloud" using newly purchased computer devices after the Sheriff of the City of New York seized plaintiff's computing devices on Tuesday, May 19, 2015. Plaintiff's then counsel represented on the record, with the plaintiff present in Court standing next to his counsel, that she "can represent on behalf of [her] client and [her] client can testify under the penalties of perjury that he has not in any way disobeyed any Court order with respect to sanitizing or destroying any sort of evidence...." Plaintiff did not object to this statement by his then counsel.

Thereafter, once the application had been fully briefed by all counsel and the Court had heard oral argument on the application the Court issued a written decision

dated September 18, 2015 (*Crocker C. v. Anne R.*, 49 Misc.3d 1202(A), 26 NYS3d 747 [Kings County]).

In the September 18, 2015 written decision the Court noted as follows:

> Defendant contends that plaintiff knew he was going to be served with the Court's May 15, 2015 order on May 18, 2015 because he was monitoring her communications using the spyware he allegedly installed on her iPhone. In support of her argument, defendant annexes copies of text messages from plaintiff to her from May 18, 2015. Plaintiff contends that he had advance notice that he was going to be served by the Sheriff of the City of New York because the sheriff "accidentally" called his cell phone to "check" if he would be home (*id* at 10).

Throughout this litigation the defendant has maintained that the plaintiff was "tipped off" that the Sheriff of the City of New York would be seizing his computing devices which gave him an opportunity to destroy incriminating evidence related to his use of spyware to surreptitiously intercept defendant's communications and monitor her location and even "listen in" on her conversations by remotely activating the microphone on her iPhone without her knowledge. Plaintiff, through former counsel on the record, conceded previously in this litigation that he received "accidental" advance notice that the Sheriff of the City of New York would be seizing his computing devices when someone called his cell phone to "check" if he would be home (*Crocker C. v. Anne R.*, 49 Misc.3d 1202(A), 10, 26 NYS3d 747 [Kings County]). Plaintiff has at no time during this litigation disputed that he had advance notice of the impending seizure of his computing devices.

Also in the September 18, 2015 decision and order, *id* at 12, the Court noted the following:

> At oral argument on June 23, 2015, plaintiff's counsel argues that there was no basis for defendant's counsel to "make an extraordinary jump from a Fifth Amendment invocation by [plaintiff]" to requesting that plaintiff's computer devices be seized. She concedes that "a negative inference flows" from plaintiff's invocation of the Fifth Amendment privilege; however, she argues that the "very limited to particular question" and not to a "whole parade of horribles [*sic*] that might be imagined or speculated to on the part of defendant." Plaintiff's counsel argued that the Court should resolve the motion by drawing a negative inference against plaintiff and the case should continue without further interruptions since, in essense, the issues of whether plaintiff installed spyware on defendant's iPhone and used it to monitor her confidential communications and location are, she posits, "in a sense, ... a collateral issue" that may only be "of some vague relevance to the question of custody or financials." Plaintiff's counsel does not address the issue of how the Court should determine the weight, if any, of the negative inference she contends should be drawn against plaintiff. Plaintiff's counsel further argued that plaintiff had legitimate sources for the information he used in litigating the pending proceeding. The Court inquired of plaintiff's counsel on the record on June 23, 2015 as follows:
>
> THE COURT: Is your client prepared today under oath to state that he's not – – under oath in open court, that he has not intercepted or seen or had any opportunity to review any confidential communications between the defendant and anyone else of a privileged nature? And if you can't answer the question now, don't because you may be bound by it.
>
> MS. BYRNE: Right. In connection with Fifth Amendment invocation – –
>
> THE COURT: I asked you a direct question. Is he willing to testify under oath that he has received absolutely no confidential information or any

privileged communication from anyone or intercepted or seen or had any knowledge from by the operation of this defendant's devices, what they may be, and if, and quite frankly, he has the right to take the Fifth Amendment – –

MS. BYRNE: Of course.

THE COURT: – – to that question, as well.

Plaintiff's counsel asserted that she did not believe that plaintiff could answer the Court's question without using his Fifth Amendment privilege as a sword and a shield and she argued that the Court could draw an adverse inference against plaintiff on the issue but, she argued, to allow defendant access to the contents of plaintiff's computing devices would only serve to give defendant "tit for tat access" to plaintiff's attorney-client communications.

Plaintiff was represented by private counsel until November 12, 2015 when he substituted himself *pro se* by consent to change attorney.

In the September 18, 2015 decision and order the Court held that:

> ...defendant must be permitted the opportunity to examine whether or not plaintiff violated the attorney-client privilege attached to e-mails defendant exchanged with her counsel and, if he did so, whether the extent of the violation prejudiced defendant's ability to participate in this litigation on a level playing field" (*id* at 21).

This Court further found in the September 18, 2015 decision that once the extent, if any, of the plaintiff's violation of defendant's attorney-client privilege was determined, the Court could determine:

> ...the appropriate remedy whether it be an application for sanctions, an application to limit plaintiff's future discovery, an application to preclude the defendant from introducing at trial any evidence or testimony for which he cannot establish a legitimate source unrelated to any confidential communications he obtained by illegal means and/or any other remedy that may be appropriate once the facts and circumstances are known (*id*.).

A court-appointed referee – retired Appellate Division Justice Ariel Belen – was appointed on consent of the parties by order dated November 5, 2015. The appointment of an attorney-referee ensured that any privileged communications of both parties uncovered during the forensic computer examination would not be seen by the Court or the other party. Pursuant to the terms of that appointment, Private Attorney Referee (hereinafter "Referee") Belen was to

> ...conduct an *in camera* review of the contents of the cloned hard-drives and ... prepare a report on the following issues: 1) whether plaintiff used spyware from these devices and, if he did so, whether he intercepted defendant's confidential and/or privileged communications, pursuant to CPLR 4503, using said spyware; and 2) if plaintiff intercepted defendant's confidential communications using spyware whether he disseminated that content or knowledge to any third-party and, if so, to whom. In the event the referee's *in camera* review reveals that plaintiff intercepted defendant's confidential communications the referee shall include a detailed inventory of the topics of said communications in the report but shall not further reveal or disseminate the content to either party. To ensure that plaintiff's privileged communications are not compromised, the referee's report shall not include any reference or details regarding plaintiff's confidential communications, if any, present on the hard-drives unless plaintiff disseminated defendant's confidential and/or privileged communications to his own attorney (*id*. at 26).

The parties each retained their own forensic computer expert to assist them and Referee Belen, on consent, in the forensic examination of the computing devices.

Referee Belen held several conferences with the parties, counsel, and the parties' respective forensic experts to formulate the process to access the data on the computing devices. These conferences resulted in a detailed agreement between the parties, dated April 6, 2016, which the Court so-ordered on consent, that regulated the manner in which plaintiff's computing devices would be taken into possession of the forensic computer experts, cloned, analyzed and ultimately returned to plaintiff. Pursuant to that agreement, the forensic computer experts would conduct the investigation jointly and confidentially and confer solely with Referee Belen and report their findings only to Referee Belen.

On April 7, 2016, the forensic computer experts took possession of the thirteen (13) computing devices from the Sheriff of the City of New York. On April 18, 2016, a fourteenth device, which had been maintained by the Court pursuant to order dated May 20, 2015, was retrieved from the Court's vault (*see* Consent Order dated October 20, 2015).

During his review of the plaintiff's computing devices Special Referee Belen reported that plaintiff provided the passwords for ten (10) of the computing devices but that there were three (3) computing devices, including an iPhone 5, iPhone 6 and an iPad, which plaintiff asserted he could not recall the passwords. As part of the examination – on consent of the parties – an outside company was employed in an attempt to unlock those three (3) password protected devices and, as a result, two (2) of the three (3)

devices were eventually unlocked (*see* Consent Order dated January 11, 2017). Despite their efforts, the computer experts were unable to unlock the third computing device or to forensically examine and assess the contents of that device. As such, it is unknown what, if any, evidence of spyware usage and/or interception of confidential and/or privileged communications were made on that device.

Thereafter, defendant made application that her iPhone also be provided to the Private Attorney Referee and the parties' forensic computer experts for examination claiming that her computer expert had uncovered evidence of plaintiff's alleged spyware activities on her iPhone (*see* Order dated September 19, 2016). Defendant's counsel argued that there was forensic data on defendant's iPhone – a "log" – of a week of plaintiff's spyware activity which may help the forensic computer experts in their examination of the data.

Subsequently on February 17, 2016, in motion sequence #12, defendant filed an application seeking an order of the Court directing the plaintiff to aver as to whether or not he had used any additional computing devices, other than those turned over to the Sheriff of the City of New York, related to the spyware that had been destroyed, lost or otherwise not been turned over for examination. The Court issued a written decision resolving that application dated June 21, 2016, which delineated the following questions

for plaintiff to answer under oath related to the ongoing investigation of the extent of his spyware use against defendant:

> The Court finds that, under the facts and circumstances presented here, the issue of whether or not plaintiff turned over all computing devices in his possession and control in compliance with this Court's May 15, 2015 order or whether or not plaintiff destroyed or hid any computing devices in anticipation of the Sheriff of the City of New York serving the May 15, 2015 order, as directed, on May 19, 2015 are crucial questions. As such, this Court hereby conditionally grants defendant's application for an adverse inference against the plaintiff on the question of whether he destroyed and/or hid a computing device(s) that contained evidence that he used the spyware he installed on the defendant's computer to monitor her confidential communications. This finding is conditional and subject to plaintiff filing a sworn affidavit directly answering each of the following questions, or alternatively asserting his Fifth Amendment privilege against self-incrimination, under oath:
>
> 1) What, if any, computing devices were in plaintiff's possession and/or control at the time he commenced this matrimonial litigation?
>
> 2) What, if any, of the computing devices in plaintiff's possession and/or control at the date of commencement were no longer in plaintiff's possession or control as of May 18, 2015?
>
> 2A) If so, what were the facts and circumstances that resulted in each computing device no longer being in plaintiff's possession and/or control between the date of commencement and May 18, 2015?
>
> 3) What, if any, computing devices were in plaintiff's possession and/or control on May 18, 2015 that were no longer in plaintiff's possession or control as of May 19, 2015?
>
> 3A) If so, what were the facts and circumstances that resulted in each computing device no longer being in plaintiff's possession and/or control between May 18, 2015 and May 19, 2015?

> 4) From the date of commencement to the present date has plaintiff accessed spyware or any information generated from spyware using any computing device in the possession and/or control of a non-party to this action?
>
> Nothing in this order shall in any way be construed to limit plaintiff's right to invoke his Fifth Amendment privilege against self-incrimination when answering the above-detailed questions by sworn affidavit if he so chooses; however, if plaintiff invokes his Fifth Amendment privilege against self-incrimination instead of answering the above-detailed questions this Court will draw an adverse inference against him on whether he failed to turn over a computing device(s) that contained evidence that he used spyware to monitor defendant's iPhone, including any confidential communications she received.

Subsequently to the Court's written June 21, 2016 decision on motion sequences #11 and #12 which delineated those questions the plaintiff retained his second counsel – Coffinas & Lusthaus P.C., who appeared by Consent to Change Attorney dated July 1, 2016.

In response to the Court's written decision and order dated June 21, 2016 the plaintiff, who was represented by counsel at that time, filed an affidavit dated July 13, 2016 in which he averred that he had provided all computing devices in his possession or control at the time of commencement to the Sheriff of the City of New York. Furthermore, he averred that there were no computing devices in his possession and/or control on May 18, 2015 that were no longer in his possession or control on May 19, 2015. Additionally, he averred that from the date of commencement to the present date

he had not accessed spyware using any computing device in the possession or control of a non-party of the action.

Special Referee Belen issued an Interim Report, dated May 25, 2017 details, as relevant here, that:

> ...***plaintiff did in fact use spyware from his computing devices and he did intercept defendant's confidential communications*** [*emphasis added*]**.** There is no forensic evidence that he disseminated that content or knowledge to any third party. The Referee further reports that there is no forensic evidence that the plaintiff intercepted or disseminated any privileged communications of the defendant.
>
> Notably, one of the Locked Devices, a device for which plaintiff could not recall his password which nonetheless was successfully unlocked and forensically imaged, "...contain[ed] forensic evidence that a day after the issuance of the May 15, 2015 Court Order and three days prior to the seizure of Plaintiff's Computing Devices by the Sheriff, ***three (3) separate 'data wiping' programs were installed and executed multiple times on this device...***[*emphasis added*]", (Joint Interim Report, dated October 31, 2016, p.9). Moreover, the experts report that "...each of [the wipes] was executed at least once on that date. Due to the nature of these wiping utilities and the nature of what they were designed to accomplish, it is impossible to determine specifically what date, if any, may have been deleted and rendered unrecoverable by this process." (Joint Interim Report, dated October 31, 2016, p. 13). It also bears noting, in this connection, the plaintiff's iPhone 5 remains password protected and cannot be unlocked.

In his Final Report, dated July 10, 2017, Special Referee Belen reported that the computer experts uncovered forensic evidence that plaintiff installed and used OwnSpy – a spyware program that can be used to record ambient conversations wherever the iPhone is located, whether the iPhone was in use or not, on a date when the

defendant's iPhone was in the "geographic vicinity of the Defendant's attorney's office according to GPS data from the Defendant's iPhone." Defendant alleges, and the data records uncovered by the forensic computer experts show, that in addition to "listening in" on her attorney-client meeting with her counsel on October 27, 2014 the plaintiff also used the spyware to "listen in" on a treatment session between her and her psychiatrist. Defendant contends that plaintiff purposefully listening in on these meetings. She argues that plaintiff specifically activated the microphone feature of the spyware to listen in on these meetings because he knew from using spyware where she would be – from using spyware to read her calendar – and when she arrived at these meetings – from using spyware to monitor her real-time whereabouts using the GPS tracking feature on her iPhone.

Upon completion of the forensic investigation of the computing devices the defendant's counsel filed this motion (motion sequence #25).

This Application

In his affirmation in support of defendant's order to show cause, defendant's counsel argues that on the day after the Court signed plaintiff's May 15, 2015 *ex parte* application the plaintiff "frantically erased what was on the device, utilizing three different 'scrubbing' devices 'multiple times' (a clear violation of the anti-spoliation orders) that he removed the most damning evidence that he obtained illegally and

surreptitiously rather than the less incriminating material." He further contends that plaintiff "utilized the remote audio functions of spyware to violate the rights of the Defendant, her psychiatrist, and myself." Referencing the Joint Interim Report of Experts dated December 30, 2016, defendant's counsel contends that, among others, plaintiff "bugged" the conversations between defendant and himself which, he asserts, violated the defendant's attorney-client privilege. The Joint Interim Report dated December 30, 2016 details that "...the log files discovered on the Defendant's iPhone covered the time period from October 25, 3014 to October 31, 2014 and contained over 7,000 pages of data [***emphasis in affidavit***]".

Defendant's counsel avers that he and his client exchanged "between 130 and 140 e-mails" between October 6, 2014 and January 3, 2015 corresponding to the three (3) month subscription that plaintiff initially purchased for iSpy, one of the multiple spyware programs he purchased, installed and utilized to monitor defendant before he commenced this litigation. Defendant's counsel contends that he exchanged many more attorney-client privileged e-mails with the defendant between January 3, 2015 and February 5, 2015 when defendant's computer expert uncovered the spyware.

Defendant's counsel argues that "common sense tells us that if Plaintiff was erasing material, he would have erased the most damning, not the least damning, and his eavesdropping on both my client's psychiatrist's office and my office would be a serious

doubleheader against him if there were any 'Richter scale' to judge the awful things he did." He argues that based upon the extensive volume of privileged communications that he exchanged with the defendant during the time when plaintiff was using the spyware that those privileged communications "must have been part of what was erased, utilizing three different wiping programs multiple times."

In support of his allegation, defendant's counsel avers that on Saturday, May 16, 2015 – the next day after the Friday, May 15, 2015 *ex parte* proceeding, the "[p]laintiff activated the audio version of the spyware he had put on my client's phone..."

Defendant's counsel further argues that on October 27, 2014 the plaintiff used the microphone "listening in" feature to eavesdrop on two privileged conversations: a consultation between defendant and her counsel in this matter that took place in counsel's law offices and a treatment session between the defendant and her psychiatrist. The Court notes that the plaintiff commenced this matrimonial action on October 28, 2014, the day after he allegedly "listened in" on the defendant's attorney-client meeting. In support of his contention, defendant's counsel avers that during the defendant's deposition of plaintiff on October 14, 2016 the plaintiff repeatedly asserted his Fifth Amendment right against self incrimination in response to numerous questions regarding whether or not he used spyware to eavesdrop on the defendant on October 27, 2014.

Supporting defendant's counsel's position, the Joint Interim Report of the forensic computer experts, dated December 30, 2016, states:

> On October 27, 2014, OwnSpy Logs indicate the 'Audio Spy' feature was activated twenty five (25) times. This is a day of importance because activations occurred at times when the location data in the OwnSpy Logs corresponding to the activation of the AudioSpy feature indicates the
>
> Defendant's iPhone was in the vicinity of the Law Offices of Raoul Felder, her attorney.

Defendant's counsel argues that plaintiff's repeated refusal to answer questions related to his use of spyware, specifically as to whether plaintiff used that spyware to "listen in" on the October 27, 2014 attorney-client consultation, together with the data uncovered by the computer experts creates a "reasonable presumption that my office was eavesdropped by the Plaintiff." He contends that plaintiff's use of three (3) different forms of data wiping software only increases the likelihood that plaintiff used the spyware as alleged by defendant and that he was desperate to obfuscate the evidence of his violation of defendant's attorney-client privilege. Defendant's counsel asserts that taken together "the presumption becomes irresistible" that plaintiff's spyware use against defendant was extensive and ongoing and that he attempted to hide his acts from the defendant and the Court.

The forensic computer experts stated in the Joint Report, dated October 31, 2016, that the data that they were unable to recover – the data that plaintiff had been unsuccessful in "wiping" after the Court's May 15, 2015 order – did not reveal that

plaintiff had electronically disseminated any of defendant's communications that he intercepted using spyware to any third-parties.[4]

However, defendant's counsel argues that the lack of forensic evidence of dissemination – forwarding – of intercepted e-mails to third-parties it is not dispositive that plaintiff did not use the information he obtained unlawfully using spyware in this litigation. Defendant's counsel contends that plaintiff used spyware and the "listening in" feature to unlawfully gain information about defendant's litigation strategy and details about defendant's case and then he passed that information to his prior counsel without revealing the source – the spyware – of the information to his counsel.

In support of this allegation, defendant's counsel asserts that during plaintiff's deposition of defendant on May 8, 2015, plaintiff's counsel asked defendant a series of questions related to a potential investment opportunity discussed between defendant and a non-party, "K.H.", in October 2014. The record reflects that plaintiff installed spyware on defendant's iPhone on October 6, 2014. Defendant's counsel argues that plaintiff learned about defendant's October 2014 investment opportunity using spyware.

Defendant, in her affidavit in support dated July 11, 2017, avers to the accuracy of

[4]There is no information before the Court at this time indicating that plaintiff's prior counsel knew that plaintiff was using spyware against defendant nor does the Court find that she had any knowledge of same. Furthermore, defendant's counsel asserts that there is "no evidence and we prefer not to believe at this point that she was told of the wiretapping and that being the source of the information fed to her by the Plaintiff so that she could question my client at her deposition. The Court notes that at the time of the May 2015 deposition of defendant the plaintiff was represented by his prior counsel whom he relieved by consent to change attorney on November 12, 2015.

the information proffered by her counsel and contends that "in terms of the dissemination issues, and my being asked questions that the plaintiff's attorney could only have obtained from the plaintiff, I want to emphasize in the strongest possible way that I never told Mr. Felder, Mr. Nottes not, or course, particularly, the plaintiff, that I had any sort of interest or plan, or anything of that nature, to look at property with my friend, "K.H.". I certainly did not mention the subject matter, even remotely, to my husband, the plaintiff, nor, I am sure, did I even tell my lawyers..." She contends that plaintiff learned the substance of her conversation with "K.H." using spyware and that he then imparted the substantive information, if not the source of that information, to his attorney who used it during her deposition.

Defendant's counsel further avers that the plaintiff repeatedly asserted his Fifth Amendment right against self-incrimination when questioned during his subsequent deposition about whether he used spyware to record telephone conversations between "K.H." and the defendant related to the October 2014 opportunity.

Defendant's counsel argues that "[p]laintiff has not only put his thumb on the scales of justice. He presses down with his entire hand." He requests that the Court preclude the plaintiff from "taking any active role directly questioning, cross-examining or offering any evidence" during trial." He contends that the trial can proceed without

the plaintiff's active involvement because the Court can hear testimony from defendant and other witnesses and defendant can submit evidence.

Plaintiff, *pro se*, in his affidavit in opposition dated July 17, 2017 contends that defendant's application should be denied because of a failure "to cite any case law or statute that would support their application for total preclusion of the Plaintiff, who is *pro se* in the matrimonial action, from testifying or offering evidence in the pending custody trial or any eventual trial on financial matters." Plaintiff further argues that "[t]he proposed relief would amount to a gross violation of due process as protected by both the 5th and 14th Amendments of the United States Constitution." Plaintiff's asserts that the Referee's Final Report exonerates him of the allegation that he used spyware against defendant because there was no forensic evidence that the plaintiff intercepted or disseminated any privileged communications by the defendant. He also contends that the relief requested by defendant must be denied because she did not "identify any confidential communications in which any such plans or investments might have been discussed with "K.H." [REDACTED BY COURT] or other parties that could have been intercepted by anyone" nor did she "identify how such information could have placed her at a disadvantage in the matrimonial litigation." Plaintiff avers that "[d]efendant's sworn statement is false." He asserts that defendant told him "on several occasions between October 2013 and April of 2014 about her visit to a potential bar-nightclub-restaurant site

in the Red Hook area of Brooklyn that "K.H." was hoping to open with the financial assistance of [defendant] as well as other unspecified investors." Plaintiff also avers that "K.H." told him directly about his interest in opening an investment with the defendant.

Plaintiff contends that the "most charitable interpretation for [defendant's] false sworn statement is that during the period in question she was usually deeply inebriated when the couple had their discussions after the children had gone to bed" and that it is "possible that she simply forgot just how forthcoming she was" during those discussions.

Plaintiff's affidavit is strikingly silent regarding the forensic computer experts' finding that he used multiple forms of data wiping software in an attempt to remove any evidence of his use of spyware. Plaintiff's affidavit is also silent on the issue of how, if at all, his repeated efforts to "wipe" his computing devices of any evidence of his spyware impacts his argument the Court should exonerate him from any finding of wrongdoing on the basis, as he argues, that the forensic examination did not uncover copies of defendant's privileged communications on his computing devices. Plaintiff does not assert that he did not use the spyware as alleged by defendant rather he contends that there should be no repercussions because the forensic computer experts were unable to find any data evidencing his spyware usage to intercept defendant's attorney-client privileged communications after plaintiff used multiple data wiping software programs to erase that data. The Court notes that the reference to the Private Attorney Referee

required him to differentiate between confidential communications – between defendant and others including her friends and family – and privileged communications – between defendant and her counsel, which are protected by the attorney-client privilege, and defendant and her psychiatrist, which are protected by the doctor-patient privilege.

Remarkably, plaintiff argues that any spoliation of electronic evidence referenced in the preliminary conference order, dated February 13, 2015, only applies to "issues in this litigation" and, he contends, that the "allegations of intercepting privileged communications did not become an issue in this trial prior to the service of the *ex parte* decision and order on May 19, 2015" and therefore his destruction of the evidence using wiping software on May 16, 2015 is inconsequential.

Defendant's counsel avers in his reply dated July 20, 2017 that "plaintiff knew fully well in advance that the Sheriff was coming to his house to seize his computing devices" after the May 15, 2015 *ex parte* order was signed by the Court. Defendant's counsel has repeatedly asserted during this litigation that on Saturday, May 16, 2016 plaintiff learned about the *ex parte* May 15, 2015 order and that the Sheriff of the City of New York had been directed to seize his computing devices on Monday, May 18, 2015 because plaintiff, who previously in this litigation conceded this point when he was represented by his first counsel, received an inadvertent telephone call from someone from the Office of the Sheriff of New York which put him on notice of the impending

seizure of his computing devices. It cannot go unnoticed that plaintiff's first counsel, while the plaintiff was present standing next to her, represented on the record that the plaintiff received inadvertent advance notice from someone at the Office of the Sheriff of New York City and plaintiff has at no time disputed his former counsel's representation.

Defendant's counsel, in his reply affirmation dated July 20, 2017, argues that "[p]laintiff's claim that there is no evidence to support defendant's position that he is guilty of the spoliation of evidence is specious." He argues that the three (3) separate data wiping programs used multiple times by the plaintiff on Saturday, May 16, 2015 to erase any spyware data from his devices was to ensure that no one could retrieve that data – the evidence of his spyware usage – demonstrates that the plaintiff used the spyware as alleged and that he was desperate to prevent the defendant and the Court from having evidence of the extent of his spyware use against the defendant. Defendant's counsel contends that because of the plaintiff's repeated, purposeful efforts to wipe the spyware data from his computing devices on Saturday, May 16, 2015 it became "impossible for anyone to determine what was deleted..." He argues that the remaining spyware data that was uncovered by the forensic computer experts on plaintiff's computing devices despite plaintiff's attempts to completely wipe the devices was just "bits and pieces that survived" and was "just the tip of the iceberg" of what would have been uncovered if plaintiff had not destroyed evidence using the three (3) wiping software programs.

Defendant's counsel argues that "plaintiff has gone beyond bad faith" and that he:

> ...intentionally and willfully defied this Court's directives to preserve evidence by using three separate softwares [*sic*] to wipe his computing devices of the damning and illegal intercepts he perpetuated against the defendant. This was not negligence by the plaintiff. This was the intentional destruction of key evidence by him.

In the Joint Interim Report dated October 31, 2016 the computer forensic experts detail the significance of data wiping as follows:

> …Deleting a file from a computer does not actually 'erase' the file from the hard drive. Deleting a file merely designates the space occupied by that file as free. Until another file is saved over that space which is occupied by the deleted file, this 'overwriting' the deleted file, the deleted file can be easily recovered using basic forensic tools. Wiping is a process by which a utility (software program) or some other method is used to 'overwrite' all of a portion of the 'free space' on [*sic*] hard drive, where among other things, all deleted files (not already overwritten through the normal operation of the computer) are overwritten with new data to ensure that any previously deleted files or data, not already overwritten, cannot be recovered.

Furthermore, the computer forensic experts detail in the Joint Interim Report dated October 31, 2016 that:

> …the forensic evidence recovered from Plaintiff's Computing Device 010 clearly shows that the wiping utilities Free File Shredder, Disk Scrubber and MariusSoft Disk Scrubber were installed on this device on May 16, 2015 and each of them was executed at least once on that date. Due to the nature of these wiping utilities and the nature of what they are designed to accomplish, it is impossible to determine specifically what data, if any, may have been deleted and rendered unrecoverable by this process.

Defendant's counsel asserts that plaintiff's claims "become more egregious" because plaintiff invoked his Fifth Amendment when questioned under oath on October 14, 2015 about whether he spent any monies to eavesdrop on a session that defendant had

with her psychiatrist and he again invoked his Fifth Amendment right in response to questions as to whether "he was present, physically, digitally or otherwise when defendant met with her attorneys at their offices on October 27, 2014." He argues that the "sole adverse inference to be drawn from just those two instances is that plaintiff did eavesdrop on a session between the defendant and her psychiatrist and did eavesdrop on a meeting with her attorney." He further argues that the same adverse inference is true with respect to plaintiff's invocations concerning his intercepting of the defendant's phone calls. Defendant's counsel argues that while no forensic evidence of these two events was present on the computing devices that plaintiff turned over to the Sheriff of the City of New York "the only conclusion that anyone can reach" is that plaintiff wiped those computing devices of all forensic data evidence of his eavesdropping on the privileged meetings between defendant and her attorneys and also with her psychiatrist. In support of his position, defendant's counsel asserts that the log files uncovered by the forensic computer experts on defendant's iPhone, which as part of the software design only stored a seven (7) day log before self-deleting and generating a new seven (7) day log, revealed that plaintiff intercepted defendant's privileged communications on at least one occasion in the only log file available. Defendant's counsel asserts that "while the log files from the previous thousand days are not available, it is safe to infer that those log files would have shown similarly surreptitious electronic eavesdropping by plaintiff."

Defendant's counsel also asserts that the forensic experts discovered that the voice intercepts perpetuated by the plaintiff using OwnSpy were wiped. He argues that "[p]laintiff, by his actions created the situation in which the sole inference to be drawn is that he persistently and for a substantial period of time illegally eavesdropped on all the defendant's communications" including all of her privileged communications both electronic and in-person meetings. The record reveals that the spyware plaintiff used gave him full remote access to the defendant's iPhone including her calendar, contacts, GPS location in real time, e-mails, text messages, phone calls and voice mail messages and the ability to "listen in" on any ambient conversations taking place around the iPhone whenever plaintiff remotely activated the microphone on the defendant's iPhone.

Defendant's counsel asserts that because plaintiff allegedly could not remember the password for one of the computing devices and the forensic computer experts were unable to unlock that device it is impossible to know "anything regarding the contents" of that device. This is particularly relevant, he argues, because that "locked" device – the iPhone plaintiff was using contemporaneously to when he was using spyware against defendant – would have been "the most relevant one" of all the computing devices turned over by plaintiff for examination. Defendant's counsel questions plaintiff's purported inability to remember his password for what defendant's counsel believes was the most

relevant device and argues that plaintiff's lack of recall is contrived and a purposeful effort to interfere with the forensic computer examination.

The attorney for the children takes the position that "[p]laintiff's surreptitious installation of spyware on his wife's phone is reprehensible, repugnant and creepy." She argues that there should be "grave consequences in this litigation and beyond." She supports defendant's application to fully preclude plaintiff from participation in the trial on financial issues. She does not support precluding plaintiff from participating in the custody trial. The Court notes that the plaintiff was permitted to fully participate in the custody trial, which has now concluded and is *sub judice*, because the Court determined that the children's best interest must take precedence over any punishment of the plaintiff for any wrong doing and the Court's determination that it would not be able to consider "the totality of the circumstances" without the evidence and testimony presented by plaintiff in a custody trial (*see Friederwitzer v. Friederwitzer*, 55 NY2d 89, 447 NYS2d 893 [1982]). The Court notes that the right to custody and parenting time is also a right of the children so to preclude the plaintiff on the issues of custody and parenting time would, in effect, punish the children for the acts of the parent.

At oral argument defendant's counsel argued that plaintiff "has hopelessly tainted this entire litigation...." because he knowingly and purposefully destroyed evidence when he used multiple software programs to "wipe" his computing devices so that it would be

impossible for anyone to know the full extent of the privileges he violated when he used spyware against the defendant.

The attorney for the children requested at oral argument that if the Court found plaintiff in contempt for his actions and violations of court orders that plaintiff only be incarcerated "during the weekends...or during the time when the children are with their mother..." so as not to deprive the children of their right to access to their father.

THE LAW

Fifth Amendment: Drawing of the Adverse Inference

Article 1 §6 of the New York State Constitution states that, "No person...shall...be compelled in any criminal case to be a witness against himself or herself..." This language is substantially identical to that of the Fifth Amendment of the United States Constitution, "No person...shall be compelled in any criminal case to be a witness against himself" (US Const amend. V, full text). A party to a civil suit may also take advantage of the Fifth Amendment, "...since the test is whether the testimony might later subject the witness to criminal prosecution, the privilege is available to a witness in a civil proceeding, as well as to a defendant in a criminal prosecution" (*Lefkowitz v Cunningham*, 431 US 801, 805 [1977]; however in the context of a civil action, a witness' Fifth Amendment privilege is more constrained:

> Unlike his counterpart in a criminal prosecution, the defendant in a civil suit has no inherent right to remain silent or, once on the stand, to answer only those inquiries which will have no adverse effect on his case. Rather,

> he must, if called as a witness, respond to virtually all questions aimed at eliciting information he may possess relevant to the issues, even though his testimony on such matters might further the plaintiff's case. (*McDermott v Manhattan Eye, Ear and Throat Hosp.*, 15 NY2d 20, 28 [1964].)

Furthermore, a party who invokes the Fifth Amendment privilege in a civil action may be subject to an adverse inference:

> In New York, unlike the rule in a criminal case, a party's invocation of the privilege against self-incrimination in a civil case may be considered by the finder of the facts in assessing the strength of the evidence offered by the opposing party on the issue which the witness was in a position to controvert (citation omitted) (*Kuriansky v Bed-Stuy Health Care Corp*., 135 AD2d 160, 178-79 [2d Dept 1988] affd, 73 NY2d 875 [1988]).

The Court of Appeals has held that when a witness invokes the Fifth Amendment in a civil action the Court may draw an adverse inference against that party (*see El-Dehdan v El-Dehdan*, 26 NY3d 19, 19 NYS3d 475 [2015] (affirming that in a matrimonial action the Supreme Court was correct to draw an adverse inference against the defendant in a contempt hearing where the defendant invoked his Fifth Amendment privilege).

The New York Court of Appeals has held that drawing the adverse inference against a party based on invocation of the Fifth Amendment privilege is "...akin to that arising when a party fails or refuses to produce a material witness who is within his

control..." (*Marine Midland Bank v John E. Russo Produce Co., Inc*., 50 NY2d 31, 42, 427 NYS2d 961 [1980]).

Attorney-Client Privilege

CPLR 4503 (a) states that a privilege exists for confidential communications made between attorney and client in the course of professional employment and CPLR 3101 (b) vests privileged matter with absolute immunity. There is a strong public policy surrounding the privilege of attorney-client communications. The New York Court of Appeals has stated that attorney-client privilege is the oldest among common-law evidentiary privileges and is intended to foster the open dialogue between lawyer and client that is deemed essential to effective representation (*see Spectrum Systems Intern. Corp. v. Chemical Bank*, 78 NY2d 371, 575 NYS2d 809 [1991]). In *People v. Shapiro*, the Court of Appeals in ruling on the sanctity of the attorney-client privilege found that "[a]ny other policy than strict inviolability, unless expressly waived, would seriously hamper the administration of justice..." (308 NY 453, 459, 126 NE2d 559 [1955]).

The Supreme Court of the United States has held that the attorney-client privilege protects confidential communications whether made by client to attorney and by attorney to client (*Upjohn Co. v. United States*, 449 U.S. 383, 389, 101 S.Ct. 677, 682 [1981]). A fundamental requirement of the attorney-client privilege is a showing that the client intended the communication with counsel to be confidential (*see People v. Harris*, 57

NY2d 335, 343, 456 NYS2d 694 [1982]). The privilege "depends on whether the client had a reasonable expectation of confidentiality under the circumstances" (*People v. Osorio*, 75 NY2d 80, 84, 550 NYS2d 612 [1989]). As long as there was a reasonable expectation of confidentiality e-mail communications between client and attorney are, like any other communication between client and attorney, protected by the attorney-client privilege (*see Willis v. Willis*, 79 AD3d 1029, 914 NYS2d 243 [2 Dept.,2010]; *see also Parnes v. Parnes*, 80 AD3d 948, 915 NYS2d 345 [3 Dept.,2011]).

It is well-established in New York that a violation of the attorney-client privilege can result in drastic remedies, including dismissing a complaint pursuant to CPLR 3103(c), which provides:

> Suppression of information improperly obtained.
>
> If any disclosure under this articles has been improperly or irregularly obtained so that a substantial right of a party is prejudiced, the court, on motion, may make an appropriate order, including an order that the information be suppressed.

In *Lipin v Bender*, the Court of Appeals found that it was a proper exercise of the trial court's discretion to dismiss the plaintiff's complaint, pursuant to CPLR 3103(c), as a remedy for her secretly reading, taking, photocopying, and retaining the defendant's attorney's confidential and privileged documents (644 NE2d 1300, 620 NYS2d 744 [1994]) finding that the statute confers "authority to do exactly what the statute says –

that is, to enter *any* order, including an order of dismissal, that is appropriate in the circumstances [*emphasis in original*]" (620 NYS2d at 747).

Spoliation

Blacks Law Dictionary defines spoliation as "[t]he intentional destruction of evidence…or the significant and meaningful alteration of a document or instrument" (6th ed. 1990) (*citation omitted*). It has long been the rule that spoliators should not benefit from their wrongdoing, as illustrated by "that favourite [*sic*] maxim of the law, *omnia presumuntur contra spoliatorem*" (1 Sir T. Willes Chitty, et al., Smith's Leading Cases 404 [13th ed. 1929]; *see West v. Goodyear Tire & Rubber Co.*,167 F.3d 776 [2nd Cir.]; *Kronisch v. US*, 150 F.3d 112, 126 [2d Cir., 1998]). This, more colloquially stated, amounts to "spoliator beware" and spoliation sanctions are appropriate where a litigant – even a future litigant – intentionally or negligently disposes of evidence before his or her adversary has an opportunity to inspect it.

New York State recognizes a broader definition of spoliation than the common law. The case law in New York relating to spoliation includes the losing, discarding or giving away of evidence by broadly defining spoliation that includes the destruction or significant alteration of evidence or the failure to preserve property for another's use as evidence in pending litigation and even before litigation is commenced where that litigation is "reasonably foreseeable" (*see VOOM HD Holdings LLC v EchoStar Satellite*

LLC, 93 AD3d 33, 939 NYS2d 321 [1 Dept.,2012]. In *VOOM*, the Appellate Division, First Department held that once a party "reasonably anticipates litigation" it must, at a minimum, institute an appropriate litigation hold to prevent the routine destruction of electronic data (*id*).

This duty to preserve key evidence, even prior to the commencement of litigation, is well-established in New York (*see also DiDomenico v. C & S Aeromatik Supplies, Inc.*, 252 AD2d 41, 682 NYS2d 452 [2 Dept.,1998]). In *DiDomencico*, the Appellate Division, Second Department held that spoliation remedies are appropriate "even if the destruction occurred through negligence rather than wilfulness, and even if the evidence was destroyed before the spoliator became a party, provided it was on notice that the evidence might be needed for future litigation" (*DiDomenico v. C & S Aeromatik Supplies, Inc.*, 252 AD2d 41, 53, 682 NYS2d 452 [2 Dept.,1998]; *see Thornhill v. A.B. Volvo*, 304 A.D.2d 651, 757 N.Y.S.2d 598 [2 Dept.2003]) [holding that a party is responsible for preserving evidence when they are on notice that it may be needed for litigation]; *see also Ortiz v. Bajwa Dev. Corp.*, 89 A.D.3d 999, 999, 933 N.Y.S.2d 366 [2 Dept.2011] ("The court may, under the appropriate circumstances impose a sanction even if the destruction occurred through negligence rather than wilfulness, and even if the evidence was destroyed before the spoliator became a party, provided it was on notice that the evidence might be needed for future litigation."); *see also Scarano* at 750, 868

N.Y.S.2d 147). The responsibility to preserve evidence that a party is on notice may be needed for future litigation is so strong that it may extend to items that are not even in the possession of the party when that party negligently fails to take steps to assure its preservation (*Amaris v. Sharp Electronics Corp.*, 304 A.D.2d 457, 758 N.Y.S.2d 637 [1 Dept.2003]).

Once the Court determines that a party had an obligation to preserve evidence and that the party spoliated the evidence the Court must apply the appropriate remedy molded to serve the prophylactic, punitive and remedial rationales underlying the spoliation doctrine. The appropriate remedy should be designed to deter parties from engaging in spoliation; place the risk of an erroneous judgment on the party who wrongfully created the risk by engaging in spoliation; and to restore the prejudiced party to the same position – to level the playing field -- he or she would have been in absent the wrongful destruction of evidence by the opposing party.[5]

It is well-established that "[t]he Supreme Court has broad discretion in determining what, if any, sanction should be imposed for spoliation of evidence" (*Ortiz v. Bajwa Dev. Corp.*, 89 A.D.3d 999, 999, 933 N.Y.S.2d 366 [2 Dept.2011]; *Scarano v.*

[5] New York State does not recognize a separate tort for spoliation for parties to litigation, instead, the Courts rely on remedies such as adverse inference instructions, preclusion and striking of pleadings (*see generally Metlife Auto & Home v. Joe Basil Chevrolet, Inc.*, 753 N.Y.S.2d 272, 282 [4th Dept., 2002] (declining to recognize a cause of action for spoliation of evidence and, instead, relying on "the comparative advantages of remedying any injury through the imposition of carefully chosen and specifically tailored sanctions….")

Bribitzer, 56 A.D.3d 750, 868 N.Y.S.2d 147 [2 Dept.2008]; *De Los Santos v. Polanco*, 21 A.D.3d 397, 799 N.Y.S.2d 776 [2 Dept.2005]).

Historically, New York courts have applied strong spoliation sanctions even for inadvertent, negligent spoliation of evidence. In *Kirland v New York City Hous. Auth.*, the Appellate Division, First Department held that dismissal of the case was appropriate where the spoliation was intentional or negligent (236 AD2d 170, 666 NYS2d 609, 611 [1 Dept.,1997]; *see also Standard Fire Ins. Co. v Federal Pacific Elec. Co.*, 14 AD3d 213, 786 NYS2d 41 [1 Dept.,2004]). In *Kirkland*, the Appellate Division, First Department found that the severe sanction of dismissal was appropriate on the basis of the patent "unfairness (in) allowing a party to destroy evidence and then to benefit from the conduct or omission" (666 NYS2d at 611).

The Court of Appeals in *Ortega v City of New York*, citing favorably to the *Kirkland* and *Standard Fire Ins. Co.* decisions, held that:

> New York courts therefore possess broad discretion to provide proportionate relief to the party deprived of the lost evidence, such as precluding proof favorable to the spoliator to restore balance to the litigation, requiring the spoliator to pay costs to the injured party associated with the development of replacement evidence, or employing an adverse inference…Where appropriate, a court can impose the ultimate sanction of dismissing the action or striking responsive pleadings, thereby rendering a judgment by default against the offending party (9 NY3d 69, 75, 845 NYS2d 773 [2007]).

Recently, in 2015, the New York Court of Appeals in *Pegasus Aviation I, Inc. v.*

Varig Logistica S.A., adopted the standards set forth by the Appellate Division, First Department in the *VOOM* decision holding that a party seeking sanctions for spoliation of evidence must show: (1) that the party having control over the evidence possessed an obligation to preserve it at the time of its destruction, (2) that the evidence was destroyed with a "culpable state of mind," which would include negligence, and (3) that the destroyed evidence was relevant to, or would have supported, the seeking party's claim or defense (26 NYS3d 543, 26 NYS3d 218 [2015]).

In addressing the second prong of the test in *Pegasus* the Court of Appeals held that if the evidence is determined to have been "intentionally or willfully destroyed" then the relevancy of that evidence to the seeking party's claim is presumed under the third prong of the inquiry (*id.* at 547).[6]

Certainly, while the determination of the appropriate sanction is within the discretion of the trial court the Court of Appeals in *Pegasus* made it abundantly clear that one of the key distinctions to guide the trial court is whether the destruction of evidence deprives the other party of the ability to establish his or her defense and whether the destruction of evidence was in bad faith.

Evidence can be spoliated along a full range of state of mind culpability:

[6] If the Court determines that the spoliation of evidence was "negligent" the party seeking spoliation sanctions must establish that the destroyed materials were relevant to their claim or defense (*id.* at 547-48; *see also Atiles v Golub Corp.*, 141 AD3d 1055, 36 NYS3d 533 [3 Dept.,2016] (court applied *Pegasus* and ruled that video footage sought "was not 'relevant to [plaintiffs'] claim…'" after determining that "plaintiffs failed to prove that defendants intentionally or willfully destroyed [portion of] video while under obligation to present it…").

innocently, negligently, recklessly, intentionally, or in bad faith. A review of the New York case law related to the remedies correlating to the state of mind of the spoliator support a general approach that as the culpability of the spoliating party decreases (from bad faith and intentional to negligent and unintentional) so too does the appeal of the punitive and deterrent purpose underlying the spoliation doctrine. The rational is obvious: where a party intentionally destroys evidence the conduct raises a strong inference that the party thought the evidence would be so harmful to its case that the risk of getting caught destroying the evidence outweighed the risk of the opposing party obtaining the evidence and the possibility that the Court could have the evidence to consider. It appears that the Court of Appeals decision in *Pegasus* intended to draw the distinction in a way that corresponds the sanction to the intent of the spoliator when possible so that less drastic sanctions are possible for spoliators who were not acting in bad faith so long as the spoliation did not result in insurmountable prejudice to the innocent party (26 NYS3d 543, 26 NYS3d 218 [2015]).

Sanctions pursuant to spoliation doctrine is the Court's attempt to place the innocent party in the same position he or she would have been in had the evidence not been destroyed by the offending party. Before the Court of Appeals decision in *Pegasus*, the case law focused more on whether the spoliated evidence would have been relevant to the contested issue, i.e. the relationship between the destroyed evidence and the claim or

defense presented by the innocent party on the theory that if there was no showing of prejudice based upon the destroyed evidence then there is no basis for sanction even if there was spoliation (*id*.). That task, of course, is unavoidably imperfect because, in the absence of the destroyed evidence, any court could only surmise with varying degrees of confidence as to what that missing evidence may have revealed. The Court of Appeals decision in *Pegasus* greatly narrowed the inquiry focusing on whether spoliator's conduct was intentional and presuming the relevance based upon the intentional conduct (*id*.). Based upon whether the spoliator's conduct was unintentional, negligent, intentional or in "bad faith" the Court can determine the appropriate remedy. Common spoliation remedies available to the trial court are the drawing of the adverse inference, issue preclusion, striking of pleadings and, in the most egregious cases, dismissal of the action.

Spoliation: Adverse Inference

Arguably the least severe sanction for spoliation of evidence in New York case law is the drawing of an adverse inference. This remedy is often applied when the Court determines that dismissal would be too severe a sanction.

In practice, when an adverse inference is drawn based upon spoliation, the Court presumes that the destroyed evidence, if produced, would have been adverse to the party that destroyed it. One of the earliest and most-cited decisions to recognize the adverse inference instruction was *Armory v. Delemirie*, 93 Eng. Rep. 664 (K.B. 1722). In that

case, a chimney sweep – Armory – found a ring with a jewel and asked a jeweler – Delemirie – to appraise its value. The jeweler returned the ring to the chimney sweep but had removed the jewel, claiming at trial that the jewel had been misplaced. The court held that unless the jewel was produced, the jury could presume it to be of the highest value possible for its size. The court, then, assumed that the jeweler would have produced the jewel had it been less valuable. This places the onus on the party who is not producing the evidence.

The adverse inference is intended to have remedial, punitive and deterrent objectives: the remedial effect is designed to restore the prejudiced party to its previous position, as if the spoliation had not occurred and the punitive and deterrent effect is supposed to discourage and punish spoliation by placing the risk of an erroneous judgment on the party who wrongfully created the risk by destroying the evidence.

Spoliation: Preclusion of Testimony and Evidence

Preclusion of evidence and/or testimony may be appropriate when the missing evidence does not deprive the moving party of the ability to establish his or her defense, and when the responsible party did not lose evidence intentionally or in bad faith (*see De Los Santos* at 398, 799 N.Y.S.2d 776; *see also Scarano* at 750, 868 N.Y.S.2d 147; *Mylonas v. Town of Brookhaven*, 305 A.D.2d 561, 563, 759 N.Y.S.2d 752, 754 [2 Dept.2003]). In situations of negligent destruction of evidence, where there was no "bad

faith" on the part of the spoliator, the Court must consider the prejudice resulting from spoliation in determining what type of sanctions are warranted (*see Scarano* at 750, 868 N.Y.S.2d 147; *Mylonas* at 563, 759 N.Y.S.2d 752).

Spoliation: Striking Pleadings

One of the most drastic remedies for spoliation, short of dismissing the action, is the striking of pleadings. "When a party negligently loses or intentionally destroys key evidence, depriving the non-responsible party from being able to prove its claim or defense, the court may punish the responsible party by the striking of its pleading" (*Baglio v. St. John's Queens Hosp.*, 303 A.D.2d 341, 342, 755 N.Y.S.2d 427 [2 Dept. 2003]; *see also Foncette v. LA Express*, 295 A.D.2d 471, 472, 744 N.Y.S.2d 429 [2 Dept.2002]). Even before the Court of Appeals decision in *Pegasus*, the case law in New York is well-established that it is within the trial court's discretion to strike pleadings when key evidence was destroyed (26 NYS3d 543, 26 NYS3d 218 [2015]). In *DiDomenico* the Appellate Division, Second Department held that separate and apart from the traditional CPLR 3126 sanctions "is the evolving rule that a spoliator of key physical evidence is properly punished by the striking of its pleading" (*DiDomenico v. C & S Aeromatik Supplies, Inc.*, 252 AD2d 41, 53, 682 NYS2d 452 [2 Dept.,1998]). In fact, the Appellate Division, Third Department has also held that the trial court properly dismissed a case where a party negligently disposed of evidence before the adversary had an opportunity to inspect it and that the spoliation need not be intentional or in bad faith

before imposing the ultimate sanction of dismissing the suit (*see Cummings v Central Tractor Farm & Country Inc.*, 281 AD2d 792, 722 NYS2d 285 [3 Dept.,2001]; leave to appeal dismissed, 96 NY2d 896, 730 NYS2d 792 [2001]).

THE FINDINGS

The record before the Court, after more than two (2) years of litigation related to the issue of spyware (which included the parties' hiring forensic computer experts and the appointment of the private attorney-referee to supervise the examination and to shield the Court and opposing party and her counsel from any attorney-client privilege communications of either party and their counsel that were uncovered during the examination) reveals that after plaintiff installed multiple sophisticated spyware applications on the defendant's iPhone and that he used that spyware to purloin the defendant's communications – including hundreds of attorney-client e-mails between her and her counsel in this action – as well as to monitor her physical location using her iPhone's global position system capabilities, for months in real-time. The record before the Court reveals that plaintiff installed spyware in early October 2014 and that defendant did not uncover the spyware until February 6, 2015.

The forensic examination of the plaintiff's computing devices revealed that he actively used the spyware programs he installed on defendant's iPhone to intercept defendant's e-mails, text messages, record her phone conversations and voice mails and track her GPS location. The forensic computer experts uncovered approximately forty-

one (41) e-mail communications from plaintiff to technical support for the spyware companies dating as early as June 29, 2012 through October 31, 2014 requesting assistance in activating and using different features of the spyware. Furthermore, plaintiff used features of that spyware – including AudioSpy – to activate the microphone on defendant's iPhone to listen in on conversations taking place between defendant and others, including at least one attorney-client privileged consultation between defendant and her counsel in this action on October 27, 2014. This AudioSpy feature essentially allowed plaintiff to use defendant's iPhone as a remote microphone so he could "listen in" to whatever conversations were taking place in the vicinity of defendant's iPhone.

The record establishes that plaintiff knew when defendant would have her attorney-client meetings because plaintiff's spyware allowed him to access her calendar and that plaintiff purposefully activated the AudioSpy during the attorney-client meeting on October 27, 2014 attempting to gain an advantage in this litigation by learning the defendant's litigation strategy.

The Joint Report of the computer forensic experts dated December 30, 2016 details the following:

> The AudioSpy feature of OwnSpy allows an individual to activate, from a control dashboard online, a feature that turns the target device into a live microphone allowing the individual to surreptitiously listen in on conversations. This function requires the individual to log into the software's dashboard in order to activate the function. The OwnSpy logs recovered and examined from the Defendant's iPhone not only indicate activation dates and times of the AudioSpy function but also supply GPS

> coordinates corresponding to the target device's location at that time, if GPS location data is available…

The joint computer forensic experts uncovered log files from defendant's iPhone showing that plaintiff activated the AudioSpy feature to listen in on defendant seven (7) times on October 25, 2014; ten (10) times on October 26, 2014; twenty-five (25) times on October 27, 2014; fifty-nine (59) times on October 28, 2014; fifty (50) times on October 29, 2014; twenty-five (25) times on October 30, 2014; and six (6) times on October 31, 2014. The computer forensic experts were unable to uncover additional data because the log file on defendant's iPhone only preserved a seven (7) day log.

Based on the plaintiff's spoliation – his attempts to thoroughly wipe all data – evidence – of his spyware use – it is impossible for anyone other than the plaintiff to know how many of the defendant's attorney-client meetings the plaintiff "listened in" on in the months between when he commenced this litigation on October 28, 2014 – the day after he "listened in" on defendant's attorney-client meeting – and when the defendant's computer expert discovered the spyware on her iPhone in early February 2015.

Tellingly, plaintiff continues to invoke his Fifth Amendment right against self-incrimination offering no representation that the October 27, 2014 attorney-client meeting was the only meeting he listened in on before defendant discovered the spyware on her iPhone in February 2015 more than three (3) months after plaintiff commenced this litigation. Based upon plaintiff's access to defendant's calendar, his access to

AudioSpy and his conduct of seeking out and listening in on at least one of defendant's attorney-client meetings is it conceivably that plaintiff "listened in" on every attorney-client meeting defendant had with her attorneys in this action in the more than four (4) months before the spyware was discovered.

Plaintiff has consistently and vigorously invoked his Fifth Amendment privilege against self incrimination regarding any and all questions surrounding the allegations of spyware, including whether he purchased the spyware (his financial records reveal that he did) and whether he used spyware to intercept defendant's privileged communications and/or monitor her daily activities (the forensic computer examination reveals that he had that ability and that he used that ability). The joint forensic computer experts report dated December 30, 2016 reveals that plaintiff activated the AudioSpy spyware at least twenty-five (25) times on October 27, 2014 including when defendant's iPhone was in the vicinity of her attorney's office.

Plaintiff's invocation of his Fifth Amendment privilege against self incrimination related to any and all questions of alleged spyware use and any violation of defendant's attorney-client privilege posed the following questions for the Court: 1) what is the extent of the adverse inference to be drawn against the plaintiff for using the Fifth Amendment; and 2) what spoliation remedy is available to the Court to ensure that defendant's ability to participate in this litigation on a level playing field is not prejudiced.

Making the questions before the Court even more complex was the revelation by the forensic computer experts that the day after the Court issued the *ex parte* Order dated May 15, 2015 for the Sheriff of the City of New York to seize and hold the plaintiff's computing devices that the plaintiff installed at least three (3) data wiping utilities and used those utilities to delete, obscure and remove any traces of his spyware activities on his computing devices. In doing so, the plaintiff effectively destroyed the most relevant evidence available related to defendant's claim that plaintiff violated her attorney-client privilege so extensively that she can never be restored to a level playing field in this litigation.

This Court finds that the plaintiff in this action knowingly and purposefully violated the defendant's attorney-client privilege through an ongoing course of conduct of intercepting hundreds of her attorney-client communications and "listening in" on her attorney-client privileged consultations.

This Court also finds that the plaintiff in this action engaged in spoliation of evidence when he installed multiple data "wiping" applications and used them to destroy much of the spyware data on his computing devices. Spoliation of evidence is a serious offense against due process and the legal process because it greatly diminishes a party's ability to obtain justice. Here, plaintiff commenced legal action against defendant, monitored her communications and physical whereabouts in real-time using spyware,

violated her attorney-client privilege and then willfully destroyed the only remaining evidence that would reveal the extent of his violation of that privilege.

The onus was on plaintiff from the commencement of litigation to preserve evidence. Plaintiff came to Court and sought judicial intervention; however, plaintiff also attempted to "hack" this litigation and to control it using knowledge gained by "listening in" on defendant's attorney-client privileged consultations and by reading her privileged communications. Plaintiff commenced this action and he was the only party who knew about the existence of the spyware on defendant's iPhone and that he had used it to monitor defendant's communications and to "listen in" on at least one of her attorney-client meeting with her attorneys if not all of them. As such, it is clear that plaintiff was on notice that his use of spyware was directly linked to the litigation that he commenced. When plaintiff destroyed the majority of the evidence of his spyware usage on May 16, 2015 he had actual knowledge that litigation had begun – litigation he himself commenced – and was therefore bound to preserve that evidence.

In addition to plaintiff's obligation as a litigant coming to Court to seek judicial intervention to preserve evidence, this Court made repeated clear, concise and unambiguous directives about spoliation:

> (1) the Preliminary Conference Order dated January 15, 2015, which the plaintiff signed while represented by counsel, states:
>
> (b) Electronic Evidence: For the relevant periods relating to the issues in this litigation, each party shall maintain and preserve all electronic files, other data generated by and/or stored on

> the party's computer system(s) and storage media (i.e. hard disks, floppy disks, backup tapes), or other electronic data. Such items include, but are not limited to, e-mail and other electronic communications, word processing documents, spreadsheets, data bases, calendars, telephone logs, contact manager information, internet usage files, offline storage or information stored on removable media, information contained on laptops or other portable devices and network access information."

(2) in the May 15, 2015 Temporary Restraining Order:

> "ORDERED: The plaintiff shall not, until further order of the Court, authorized or direct any other individual to delete, sanitize or alter any information stored in online storage accounts, 'clouds' or any other accounts that store digital information..."

(3) in the September 18, 2015 Decision and Order states:

> "Plaintiff is reminded and cautioned that the restraining orders in this Court's May 15, 2015 order remained in full force and effect [***emphasis in original order***].

Under the facts and circumstances presented here, the Court cannot examine the issue of the plaintiff's violation of the defendant's attorney-client privilege without also examining the plaintiff's spoliation of evidence. In arriving at the appropriate spoliation sanction in this matter the Court must follow the 2015 Court of Appeals decision in *Pegasus* (26 NYS3d 543, 26 NYS3d 218 [2015]). Clearly, plaintiff was under an obligation to preserve the electronic evidence related to his spyware both at common law as a litigant seeking affirmative judicial intervention and pursuant to the Preliminary

Conference order dated February 13, 2015. As such, the first prong of the *Pegasus* test is satisfied (*id*.).

Second, plaintiff's spoliation was intentional and in bad faith. Plaintiff actively downloaded three (3) data wiping software programs and repeatedly used them in a purposeful attempt to destroy all evidence of his spyware usage. As such, the second prong of the *Pegasus* test is satisfied (*id*.). In addressing the second prong of the test in *Pegasus* the Court of Appeals held that if the evidence is determined to have been "intentionally or willfully destroyed" then the Court must draw the inference that the relevancy of that evidence to the seeking party's claim is presumed under the third prong of the inquiry (*Pegasus*, 16 NYS3d at 547). Clearly, the facts and circumstances before this Court require that the relevancy of the destroyed evidence be presumed under *Pegasus* (26 NYS3d 543, 26 NYS3d 218 [2015]).

The plaintiff's spoliation of evidence effectively obfuscated any chance for the defendant to know the extent of his violation of her attorney-client privilege and for the Court to be able to assess how much the violation may have actually prejudiced the defendant. Had the plaintiff not engaged in spoliation it is possible that once the extent of his violation of the attorney-client privilege was known that a less severe remedy may have been appropriate; however, plaintiff's purposeful spoliation of the primary evidence, together with his continued assertion of his Fifth Amendment right against self

incrimination, leave the Court with no option but to draw the most stringent of adverse inferences against the plaintiff and to consider the most drastic spoliation sanctions under *Pegasus* (26 NYS3d 543, 26 NYS3d 218 [2015]).

In this case, based upon the representations of defendant's counsel that he exchanged more than two hundred (200) e-mail communications with his client during the time period in question (October 2014 into February 2015) and the evidence discovered by the forensic computer experts that plaintiff activated AudioSpy – the "listening in" feature of the spyware – while he knew the defendant was meeting with her counsel in this matter on October 27, 2014, the Court finds that plaintiff repeatedly and purposefully violated the defendant's attorney-client privilege in the most intrusive way. Relying on that adverse inference the Court finds that plaintiff in fact read all of the more than two (200) hundred attorney-client e-mails defendant exchanged with her counsel in this action and that he listened in on any and all attorney-client meetings she had with counsel in this action during the four months between when plaintiff commenced this action in late October 2014 and early February 2015 when defendant's computer expert uncovered the spyware on her iPhone. The Court notes that the logs on defendant's iPhone just from the last week of October 2014 show that plaintiff was actively "listening in" on her conversations at times fifty (50) times a day. There is little reason to believe that plaintiff discontinued his spyware activities thereafter and, based upon plaintiff's

intentional and bad faith spoliation the Court must draw the inference that plaintiff in fact continued his course of conduct. That adverse inference must include the finding that plaintiff's violation of defendant's attorney-client privilege allowed him to obtain information that would be unavailable to him through normal methods of pre-trial discovery.

The Court notes that the timing of plaintiff's choice to engage in spoliation of evidence the very next day after the defendant went to Court to make her *ex parte* application is troubling. Plaintiff conceded in this litigation that he received advance notice on May 16, 2015 that the Sheriff of the City of New York was coming to seize his computing devices and he took that opportunity to obtain three (3) data wiping software programs and to use them all on the evening of May 16, 2015 in an attempt to cover up his conduct. Clearly, plaintiff's decision to destroy as much data evidence of his spyware usage after learning that his computing devices would be seized reveals his intent to prevent the defendant and the Court from learning the extent of his actions.

Ultimately, the source of plaintiff's advance notice that his computing devices were going to be seized imminently is inconsequential to this Court's determination of this matter. The adverse inference that must be drawn under facts and circumstances presented here and under the existing case law is that defendant's conduct in intentionally destroying evidence raises a strong inference that defendant thought the evidence would be so harmful to his case that the risk of getting caught destroying the evidence

outweighed the risk of the defendant obtaining the evidence and the possibility that the Court could have the evidence to consider. Plaintiff had a duty to preserve the evidence, he engaged in spoliation, his spoliation was intentional and in bad faith and the spoliation irreparably prejudiced the defendant in this action because she cannot be restored to a level playing field with the plaintiff.

Clearly, plaintiff's memory cannot be purged of the ill-gotten knowledge he acquired by surreptitiously "bugging" defendant's iPhone and, essentially, sitting in, uninvited, on her attorney-client consultations with counsel. Plaintiff effectively "hacked" this litigation in an attempt to hijack the legal process to gain a litigation advantage while undermining defendant's right to counsel, which includes her right to private consultation with that counsel, without any regard for the rule of law and the sanctity of the litigation process.

Plaintiff came to this Court and sought all the rights, advantages and protections of the legal process without subjugating himself to the obligations of participating in the litigation process. If the Court does not protect the integrity of the litigation process the very system for protecting the rights and due process of all litigants is compromised.

Here, the attorney-client privilege was fully and repeatedly violated. In fact, the plaintiff, when successful using an early version of spyware, subsequently installed additional versions – more sophisticated versions – of spyware to continue and to expand his intrusion into defendant's attorney-client privilege. The record reveals that plaintiff

had numerous opportunities during the months before the defendant's computer expert uncovered the spyware to minimize the prejudice to defendant by discontinuing his spyware usage but that at each juncture he chose the course of action that exacerbated the harm by increasing his intrusions using more and more sophisticated "hacking" methods. The Court notes that plaintiff did not stop using the spyware rather defendant found the spyware.

In this instance, the course of plaintiff's fate in this litigation has been established by his own considered course of conduct which he had many opportunities to rectify: the full extent of the prejudice against defendant can never be known because the plaintiff engaged in intentional, bad faith spoliation of the key evidence by painstakingly trying to delete all data evidence of his wrongful acts by attempting to "wipe" his computing devices of all traces of his spyware usage. Without the full data evidence of plaintiff's unlawful spyware usage the Court must assume, in effect, "the worst" that the record supports under *Pegasus* (26 NYS3d 543, 26 NYS3d 218 [2015]).

As such, when considering the record as a whole, the only reasonable and fair option before the Court is to implement the strongest spoliation sanction available and, also, to draw a severe adverse inference against the plaintiff, as required by his steadfast assertion of his Fifth Amendment right against self-incrimination. As such, this Court has no option under the facts and circumstances presented, and the gravity of plaintiff's acts, but to accept as true defendant's position that plaintiff not only intercepted all of her

electronic attorney-client communications – numbering more than two (200) hundred – and that plaintiff "listened in" on at least one of the defendant's consultations (on October 27, 2014) with her counsel and that he used the knowledge to his advantage in this litigation. This Court is mindful in reaching this finding that the record, together with the adverse inference, supports a finding that plaintiff "listened in" on all of the defendant's attorney-client meetings until the spyware was uncovered in February 2015.

Prejudice results when evidence obtained in violation of the attorney-client privilege is used against the violated party. Here, plaintiff gravely prejudiced the defendant. Plaintiff's contumacious conduct – his apparent belief that his personal advantage in this litigation warrant any action regardless of the lawfulness or the impact on the defendant and without any regard for the judicial process – presents the Court with the challenging task of determining the proper response and remedy to restore defendant's equal footing in this litigation.

Upon careful examination of the case law in New York related to violation of the attorney-client privilege and spoliation it appears that the facts and circumstances presented by this plaintiff's violation of the attorney-client privilege and his spoliation of evidence are unprecedented by a plaintiff in a matrimonial litigation. This Court must determine what spoliation sanction is appropriate while also taking into account the strong public policy considerations in matrimonial actions involving children, as is the case here where the parties have two (2) young children. In reaching the ultimate

determination, the Court remained mindful that any appropriate remedy must safeguard the rights of the parties' children and the parties' Constitutional rights to their children.

The Court notes that when faced with a much less egregious fact pattern the trial court in *Berliner v. Berliner* [Spolzino, J.] noted that the remedies that may be available in other types of civil litigation are not always appropriate in matrimonial actions where remedies must be balanced against strong public policy issues. In *Berliner,* a computer consultant for the wife discovered that a program known as "Home Key Logger", an early and basic form of spyware which records keystrokes a user makes on a computer, had been installed on the wife's computer without her knowledge. That key stroke data had been used so that the husband could discover the wife's passwords and have her private computer documents downloaded. In *Berliner,* the husband who had obtained the ill-gotten electronic data from the wife's computer subsequently engaged in spoliation of that evidence so that it was unclear to the Court what electronic data had been taken from the wife. The trial court found that the appropriate sanction was to preclude the husband from introducing at trial any documentary evidence for which he could not establish a legitimate source.[7]

[7]The Court notes that in the same decision the trial court found the husband in *Berliner* to be in contempt of court orders and incarcerated him for ten (10) days. One of the orders the husband violated that resulted in his incarceration was his failure to preserve the evidence of his conduct with respect to the wife's computer files where it was found that he engaged in spoliation of evidence in violation of court order subsequent to the wife's discovery that her private computer files had been compromised. The Appellate Division, Second Department affirmed the trial court's contempt adjudication (*see Berliner v. Berliner,* 33 AD3d 745, 823 NYS2d 189 [2 Dept.,2006]).

This Court notes that, in *Berliner*, the spyware was not nearly as sophisticated as the spyware used by the plaintiff in this case and, critically important, there was no allegation in *Berliner* that the electronic data take from the wife was subject to attorney-client privilege. Clearly, the actions by the plaintiff in the case before this Court present a much more egregious set of facts than those in *Berliner*. Despite the much more limited facts presented in *Berliner*, the trial court subsequently found the husband in civil contempt, pursuant to Judiciary Law 753, and he was incarcerated based upon his spoliation of the evidence of his electronic monitoring of the wife after she discovered the intrusion. The Appellate Division, Second Department affirmed the trial court's contempt adjudication inasmuch as there was a court order that the husband preserve the evidence and he did not do so (*see Berliner v. Berliner*, 33 AD3d 745, 823 NYS2d 189 [2 Dept.,2006]).

In *Matter of Weinberg*, the plaintiff's counsel employed deceitful and unprincipled means to secure discovery of confidential and privileged material from the adverse party's former law firm without notifying the plaintiff of the ill-gotten information (129 AD2d 126, 517 NYS2d 474 [1 Dept.,1987]). As a remedy, the trial court found that it would sufficiently ameliorate the prejudice to defendant for the plaintiff's counsel to be disqualified – a drastic remedy – where the plaintiff's counsel had engaged in a violation of the defendant's attorney-client privilege but the plaintiff had not been involved. The Appellate Division, First Department affirmed the trial court decision finding that

disqualification of the plaintiff's counsel from further participation in the proceeding was an appropriate and necessary remedy because there was no other way of assuring that the tainted knowledge, improperly obtained, would not subtly influence that firm's conduct of the litigation in the future. Further, the Appellate Division, First Department upheld the trial court's determination that plaintiff must establish, once new counsel was in place, an independent source for any information that may have also been discoverable through the documents improperly obtained by disqualified counsel.

Where the plaintiff is the party who violated the attorney-client privilege and the violation of the privilege was extensive the Court of Appeals has found that dismissal of plaintiff's case was the "only practical remedy" (*Lipin v. Bender*, 644 NE2d 1300, 1305, 620 NYS2d 744 [1994]). In *Lipin*, the Court of Appeals noted that dismissal was necessary because "the wrongdoing and the knowledge were the client's own, which she would carry into any new attorney-client relationship" (*id* at 1304).

Based upon this Court's finding that it must draw the fullest adverse inference against plaintiff, the facts presented here reveal that plaintiff's violation of privileged communications was far greater than what was alleged in *Berliner*. In *Berliner* only limited files were removed from the wife's computer on one occasion using floppy disks whereas in the case before this Court, the sophisticated spyware used by plaintiff enabled him to systematically monitor all of defendant's online activity and physical whereabouts

in real-time for at least four (4) months and to "listen in" on her attorney-client meetings with her attorney in this matter.

While this Court is deciding this application based upon the issues of spoliation and the violation of the attorney-client privilege the Court notes that the controlling case law in New York holds that a plaintiff cannot seek judicial relief while also claiming the Fifth Amendment privilege against self-incrimination which is precisely the situation that plaintiff proposes to this Court. In *Levine v Bornstein*, the trial court struck the complaint and dismissed the action, with costs, where the plaintiff refused to answer certain questions during a deposition because the questions propounded indicated that the plaintiff may be subject to a fine or imprisonment under the penal code (13 Misc.2d 161, 174 NYS2d 574 [Kings County, 1958]. The trial court noted that:

> [t]he research of the court has failed to reveal a reported case in this state wherein the plaintiff claimed the privilege. However, in *Franklin v. Franklin*, 365 Mo. 442, 283 S.W.2d 483, a divorce action, it was held that where a party invoked the jurisdiction of a court for affirmative relief, such relief may be denied if he refuses to testify upon the grounds of self-incrimination; and in *Annest v. Annest*, 49 Wash.2d 62, 298 P.2d 483, also a divorce action, it was held that where a party claims the privilege, the court may dismiss his action or strike his testimony (*id* at 164).

The trial court in *Levine* found that "[t]he plaintiff therefore obviously had the right to claim the privilege, but he cannot eat his cake and have it too" (*id* at 165) and ultimately dismissed the action. The decision and order of the trial court in *Levine* was affirmed by the Appellate Division, Second Department (7 AD2d 995 [2 Dept.,1959])

and by the Court of Appeals (6 NY2d 892 [1959]).[8] The Court notes that there are very few reported civil cases in New York addressing the issue of a plaintiff asserting the Fifth Amendment and, although it is not a recent decision, the Court of Appeals affirmation of *Levine* remains the controlling law in New York on that issue. In fact, the Court of Appeals cited favorably to *Levine* in 1979 in *Prink v Rockefeller Center, Inc*. again holding that "[c]learly his privilege against self incrimination would not have helped him, for that privilege does not permit a plaintiff to claim affirmative relief and at the same time refuse to disclose information bearing upon his right to maintain his action" (48 NY2d 309, 316 422 NYS2d 911 [1979]).[9]

The Court of Appeals has continued to uphold the principal that a plaintiff in a civil action cannot assert the Fifth Amendment privilege and also seek affirmative relief.

[8]The precedent in *Levine* has not been overturned. The Court notes that the trial court in *Castellana v New York Herald*, denying the defendant's motion to dismiss the plaintiff's complaint where there plaintiff asserted his Fifth Amendment privilege during depositions where a federal indictment was pending on the issues presented and where, the trial court found, it would not prejudice the defendant's to wait until after the federal proceeding was completed to proceed on the civil action (44 Misc2d 211, 253 NYS2d 507 [New York County, 1964]). The trial court in *Castellana* conditioned the denial on plaintiff appearing and submitting "to examination before trial, at which shall testify without claiming the privilege asserted, immediately following the completion of the trial or other disposition of the criminal proceeding in the federal court or within six months after service of a copy of the order to be entered hereon with notice of entry thereof, whichever is sooner" (*id* at 212). The facts presented in the case before this Court differ considerably from the facts in *Castellana* and, the Court notes, the holding in *Castellana* was not appealed and appears inapposite to the controlling Court of Appeals precedent.

[9] In *Prink*, a wrongful death action where circumstances of the decedent's death were consistent with their negligence, as the plaintiff claimed, or suicide, as the defendant claimed, the plaintiff, during her examination before trial, admitted that the decedent, her husband, had told her that he was seeing a psychiatrist, but refused to disclose, based on the spousal privilege, the content of that communication.

In *Steinbrecher v. Wapnick*, 24 NY2d 354, 300 NYS2d 555 [1969], the Court of Appeals, citing *Levine*, found:

> There is one important exception to the general rule that a witness is free to rely on the privilege unless he has waived it by voluntarily testifying to incriminating facts. Since the sole purpose of the privilege is to shield a witness against the incriminating effects of his testimony, the courts will not permit its use as a weapon to unfairly prejudice an adversary. (*See Levine v. Bornstein*, 6 N.Y.2d 892, 190 N.Y.S.2d 702, 160 N.E.2d 921; *Brown v. United States*, 356 U.S. 148, 155—156, 78 S.Ct. 622, 2 L.Ed.2d 589.) In the *Levine* case, 6 N.Y.2d 892, 190 N.Y.S.2d 702, 160 N.E.2d 921, *Supra*, the privilege was invoked by a Plaintiff at an examination before trial in a civil suit, with the effect of depriving the defendant of information necessary to his defense. For this reason, our court upheld an order dismissing the complaint. The considerations which motivated the court in the *Levine* case, however, have no application where the privilege is asserted by a Defendant (*id*. at 362-63).

Here, the remedy available to the Court in *Berliner v Berliner* – preclusion – is not an adequate remedy because of the extent of the plaintiff's violation of the attorney-client privilege so "poisoned" the litigation, similar to the situation presented in *Lipin v Bender*, and because based upon plaintiff's spoliation of the relevant evidence there is no practical way for the defendant or the Court to determine whether plaintiff has a legitimate, independent source of information. Certainly, the Court of Appeals, in upholding *Lipin v Bender*, *Levine v Bornstein*, and *Steinbrecher v Wapnick* has been abundantly clear that it is well within a trial court's discretion to dismiss a plaintiff's cause of action for any one of the three (3) acts [violation of the attorney-client privilege, spoliation, claiming the Fifth Amendment] that the plaintiff in this case has chosen. However, this Court finds

that, dismissal of the plaintiff's action, as was upheld by the Court of Appeals in *Lipin v Bender* (for plaintiff violation of the attorney-client privilege) and in *Levine v Bornstein* and *Steinbrecher v Wapnick* (for plaintiff claiming the Fifth Amendment privilege), is not an adequate remedy because this is a matrimonial action and to dismiss the action would prejudice the defendant's right to continue to litigate this divorce action and to obtain a divorce from the plaintiff. Furthermore, this Court notes that dismissal would be inappropriate in this matrimonial action because of the issues of custody and parenting time, which have been described as a Constitutional right. This Court finds that the appropriate remedy in this action must preserve the defendant's right to obtain a divorce in this action and the children's right for financial support and meaningful access to their father.

This Court is keenly aware that in this matrimonial action the defendant had the independent financial ability to employ and pay for forensic computer experts, to pay for the cost of a private-attorney referee and, above all, to pay for a team of experienced counsel. The Court notes that but for defendant's counsel scrupulous, "fine-tooth" examination of plaintiff's financial records it is unlikely that anyone would have uncovered the fact that plaintiff used his PayPal account to purchase spyware. The Court notes that the initial cost of the spyware was approximately $50.00; however, the cost to these parties of this litigation, the majority of which has centered around the defendant's attempt to ascertain the extent of plaintiff's violation of her attorney-client privilege and

plaintiff's corresponding recalcitrance in complying with that discovery and his active destruction of evidence, has forced the cost of this litigation well over $2,000,000 which is certainly outside of the financial means of the majority of parties who seek judicial intervention in a matrimonial action in this County. How do the Courts of this State protect those who find themselves victims of such egregious conduct but who are less financially fortunate and cannot expend the financial resources to subsidize this through a litigation? This Court finds that these victims must be protected by the imposition of the strictest of penalties possible.

Based upon the totality of the facts and circumstances, including the plaintiff's total and on-going violation of the defendant's attorney-client privilege for more than four (4) months which included purloining hundreds of her attorney-client privileged communications and "listening in" on her attorney-client meetings, together with the allegation that he also "listened in" on her sessions with her treating psychiatrist, together with his intentional and bad faith spoliation of the only evidence that would have allowed the defendant and the Court to assess the extent of any negative inference, and in the interest of justice, the Court finds that the appropriate remedy is to strike the plaintiff's pleadings related to all financial relief except for the issue of child support, which is the right of the children. The Court does not make this determination without great and thorough consideration of all of the applicable case law, including the recent Court of Appeals decision in *Pegasus*, together with all of the facts and circumstances presented.

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. The remedy in *Berliner* was sufficient given the very limited nature of the spyware intrusion where no attorney-client privilege was allegedly violated; however, here, given the complete violation of defendant's attorney-client privilege, which apparently took place daily for month, it would be impossible to parse between what information plaintiff had an independent source for and what information plaintiff was obtaining from his spyware monitoring. The Court notes that while not all civil remedies may always be appropriate in every matrimonial action that under the facts and circumstances here it would be unjust to allow the plaintiff to escape the appropriate sanctions for his conduct by hiding behind the nature of this action. Matrimonial actions remain civil actions and litigants who seek judicial intervention must comply with the rule of law. This Court will not turn a blind-eye to spoliation of this extent simply because it takes place in a matrimonial action. Spoliation of key evidence is no less prejudicial when it happens in the context of a matrimonial action. Additionally, given the extensiveness of the violation of defendant's

attorney-client privilege it is evident that plaintiff had the ability to learn defendant's counsel's litigation strategy. The readily available and sophisticated spyware available in this Internet Age to a spouse intent on wielding power over another spouse presents a new tool of control. Any litigant, intent on exercising power and control over another litigant, by installing and using spyware in an attempt to gain an advantage in a matrimonial action by violating the sanctity of the attorney-client privilege must be aware that the Court will act to protect the sanctity of the attorney-client privilege and the legal process. Litigants in matrimonial actions must abide by the same standards of conduct as those in other forms of civil litigation and intentional, bad-faith spoliation must be held to the same standards as in any other civil action.

The Court is mindful that plaintiff probably never contemplated that his initial investment of approximately $50.00 of spyware would start him on this path or have such dire consequences to his financial future; however, plaintiff's conduct in this litigation both shocks the consciousness of the Court and offends all semblance of judicial integrity that the Court is presented with little discretion in reaching this ultimate determination. The Court notes that in the years since defendant discovered the spyware on her iPhone the plaintiff has remained recalcitrant in his position and, as a result, the parties have incurred many hundreds of thousands of dollars in counsel fees, expert fees and litigation costs related solely to the issue of spyware. Now, after the full forensic examination the defendant and the Court now know what plaintiff knew all along: that plaintiff long ago

destroyed the key evidence of the extent of his spyware usage. The Court notes that this financial cost does not include the unquantifiable day-to-day cost to the parties and to their children of living through this protracted litigation.

Based upon the foregoing, this Court hereby strikes plaintiff's pleading seeking spousal support, equitable distribution and counsel fees. In considering the available remedies the Court found that merely precluding the plaintiff on the issue of equitable distribution and allowing that issue to proceed to trial given the Court's ability to consider egregious conduct in any award of equitable distribution; however, given the compounding extensive nature of the plaintiff's violation of the attorney-client privilege and his intentional and bad-faith spoliation the Court found that preclusion on the issue of equitable distribution was not sufficient and that the only appropriate remedy under the facts and circumstances presented here was to also strike plaintiff's pleadings as to equitable distribution. The Court does not strike the plaintiff's pleadings relating to any request for child support if he is awarded custody inasmuch as child support is the right of the children and it would prejudice the children to strike his request for children support if he is awarded custody. The Court notes that the issues of custody and parenting time have been tried and are *sub judice* at this time. The trial on the financial issues is scheduled to begin on Tuesday, May 1, 2018 at 2:15 p.m. The parties shall exchange last three years tax returns and statements of proposed disposition related to the issue of children support on or before April 20, 2018.

Contempt

The failure to obey a lawful order of a Court is punishable by a finding of contempt which may constitute a criminal contempt, a civil contempt, or both a criminal and a civil contempt and a period of incarceration may, based upon the facts and circumstances, be imposed upon the finding of either a criminal or civil contempt.

Judiciary Law 753, as relevant hereto, provides:

> A. A court of record has power to punish, by fine and imprisonment, or either, a neglect or violation of duty, or other misconduct, by which a right or remedy of a party to a civil action or special proceeding, pending in the court may be defeated, impaired, impeded, or prejudiced, in any of the following cases:
>
> 8. In any other case, where an attachment or any other proceeding to punish for a contempt, has been usually adopted and practiced in a court of record, to enforce a civil remedy of a party to an action or special proceeding in that court, or to protect the right of a party.

Judiciary Law 750, as relevant hereto, provides:

> A. A court of record has power to punish for a criminal contempt, a person guilty of any of the following acts, and no others:
>
> 1. Disorderly, contemptuous, or insolent behavior, committed during its sitting, in its immediate view and presence, and directly tending to interrupt its proceedings, or to impair the respect due to its authority.
>
> 2. Breach of the peace, noise, or other disturbance, directly tending to interrupt its proceedings.
>
> 3. Wilful disobedience to its lawful mandate.
>
> 4. Resistance wilfully offered to its lawful mandate.
>
> 5. Contumacious and unlawful refusal to be sworn as a witness; or, after being sworn, to answer any legal and proper interrogatory.
>
> 6. Publication of a false, or grossly inaccurate report of its proceedings. But a court can not punish as a contempt, the publication of a true, full, and fair report of a trial, argument,

> decision, or other proceeding therein.
> 7. Wilful failure to obey any mandate, process or notice issued pursuant to articles sixteen, seventeen, eighteen, eighteen-a or eighteen-b of the judiciary law, or to rules adopted pursuant thereto, or to any other statute relating thereto, or refusal to be sworn as provided therein, or subjection of an employee to discharge or penalty on account of his absence from employment by reason of jury or subpoenaed witness service in violation of this chapter or section 215.11 of the penal law. Applications to punish the accused for a contempt specified in this subdivision may be made by notice of motion or by order to show cause, and shall be made returnable at the term of the supreme court at which contested motions are heard, or of the county court if the supreme court is not in session.

In *Gompers v Buck's Stove & Range Company*, 221 US 418, 31 S.Ct. 492, the United States Supreme Court stated the following:

> Contempts are neither wholly civil nor altogether criminal. And 'it might not always be easy to classify a particular act as belonging to either one of these two classes. It may partake of characteristics of both' [citations omitted].... It is not the fact of punishment, but rather its character and purpose, that often serve to distinguish between the two classes of cases. If it is for civil contempt the punishment is remedial, and for the benefit of the complainant. But if it is for criminal contempt the sentence is punitive, to vindicate the authority of the court.... [I]mprisonment for civil contempt is ordered where the defendant has refused to do an affirmative act required by the provisions of an order which, either in form or substance, was mandating in its character. Imprisonment in such cases is not inflicted as a punishment, but is intended to be remedial by coercing the defendant to do what he had refused to do. The decree in such cases is that the defendant stand committed unless and until he performs the affirmative act required by the court's order" (*id*. at 441–442).

A party may be found in civil contempt where ordered to do something, refuses to comply and is committed to a jail term until after being found in contempt where the party may remain until they purge the contempt by complying with the original order.

For example, a parent who is found to willfully failed to pay child support and is incarcerated; the contempt is purged and the parent is released from custody when the payment of child support arrears is paid (*see generally Cutroneo v. Cutroneo*, 140 AD3d 1006, 35 NYS3d 173 [2 Dept.,2016]). In civil contempt, the civil contemnor is said to hold the keys to the prison because they have the ability to end the incarceration upon compliance with the Court's order and only remain incarcerated while they refuse to do so.

In *Gompers*, the United States Supreme Court posed the following example of criminal contempt:

> ...if the defendant does that which he has been commanded not to do, the disobedience is a thing accomplished. Imprisonment cannot undo or remedy what has been done, nor afford any compensation for the pecuniary injury caused by the disobedience. If the sentence is limited to imprisonment for a definite period, the defendant is furnished no key, and he cannot shorten the term by promising not to repeat the offense. Such imprisonment operates as a remedy coercive in its nature, but solely as punishment for the completed act of disobedience ... The distinction between refusing to do an act commanded (remedied by imprisonment until the party performs the required act), and doing an act forbidden (punished by imprisonment for a definite term), is sound in principle, and generally, not universally, affords a test by which to determine the character of the punishment" (id. at 442–443).

The New York Court of Appeals found in *Matter of Department of Envtl. Protection of City of N.Y. v. Department of Envtl. Conservation of State of N.Y.* that "[a] criminal contempt...involves an offense against judicial authority and is utilized to protect the integrity of the judicial process and to compel respect for its mandates" (70 NY2d

233, 239, 519 NYS2d 539 [1987]. When a party is incarcerated for a period of time and is unable to shorten that term by purging the contempt, the contempt is criminal: the party does not hold the keys to the prison because the party cannot shorten the period of incarceration by purging.

The Appellate Division, Second Department in *Rubackin v Rubackin* found that "[w]hen the purpose of committing an individual to jail is in the nature of vindication the authority of the court, protecting the integrity of the judicial process, or compelling respect for the court's mandates, the contempt is a criminal contempt" (62 AD3d 11, 15, 875 NYS2d 90 [2 Dept.,2009]). In order to sustain a finding of criminal contempt, there must be proof beyond a reasonable doubt that the contemnor willfully failed to obey an order of the court (*see County of Rockland v. Civil Serv. Empls. Assn.*, 62 NY2d 11, 15, 475 NYS2d 817 [1984]. "An essential element of criminal contempt is willful disobedience" (*Dalessio v. Kressler*, 6 AD3d 57, 65-66, 773 NYS2d 434 [2 Dept.,2004]).

The issue of whether plaintiff's acts of spoliation rise to the level of civil and/or criminal contempt is referred to the trial court. The Court is mindful of the strong policy of children having a right to access to their parents absent exceptional circumstances (*see generally Zafran v. Zafran*, 28 AD3d 753, 755, 814 NYS2d 669 [2 Dept.,2006]).

Plaintiff has the right to obtain counsel of his own choosing. Plaintiff has been represented by two (2) prior privately retained attorneys both of whom he discharged by filing consent to change attorneys substituting himself *pro se*. During this litigation,

defendant has provided substantial financial contribution to plaintiff's counsel fees, without prejudice, on multiple occasions. The Court notes that based upon representations of the parties during this litigation it appears that they have spent in excess of $2,000,000 to litigation this action.

This Court has repeatedly notified plaintiff on the record of his right to seek counsel of his own choosing and has provided him with lists of bar association referral panels and provided him with the location of the Office of Self Represented located in room 122-c of this courthouse. The plaintiff is not eligible for Court assigned counsel and himself earns income in excess of $100,000 annually – far in excess of the threshold for the assignment of counsel.

Conclusion

The relief requested by plaintiff in motion sequence #25 is granted to the extent detailed herein.

This shall constitute the decision and order of this Court.

ENTER:

JEFFREY S. SUNSHINE
J. S. C.