UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CATHERINE KASSENOFF, PLAINTIFF	)	
V.	)	COMPLAINT AND JURY DEMAND
ALLAN KASSENOFF, CONSTANTINE G. DIMOPOULOS, AND DIMOPOULOS BRUGGEMANN PC DEFENDANTS	)	MARCH 15, 2022

COMPLAINT

Plaintiff, CATHERINE KASSENOFF, for her Complaint for damages and injunctive relief against Defendants ALLAN KASSENOFF, CONSTANTINE G. DIMOPOULOS and DIMOPOULOS BRUGGEMANN PC states the following:

PARTIES

1. Plaintiff, Catherine Kassenoff, is a resident of Westchester County, New York.

2. Defendant, Allan Kassenoff ("Defendant"), is a resident of Larchmont, New York.

3. Defendant, Constantine G. Dimopoulos ("Dimopoulos"), is a licensed New York attorney, whose principal place of business is in Eastchester, New York and upon information and belief is a resident of Scarsdale, New York. At all relevant times herein, he served as Defendant's attorney.

4. Defendant, Dimopoulos Bruggemann PC, ("the Firm"), is upon information and belief, a corporation organized under the laws of the state of New York, which provides legal services to clients through its individual shareholders, members, agents and/or employees. Upon

further information and belief, the Firm is owned, controlled, and managed, wholly or in part by Dimopoulos who provides matrimonial litigation services to clients through the Firm.

JURISDICTION AND VENUE

5. This Court has jurisdiction under 28 U.S.C. § 1331 based upon the Defendants' violations of Title 3 of the Omnibus Crime Control and Safe Streets Act of 1968, specifically: 18 U.S.C. § 2510 *et seq*., and/or, 18 U.S.C. § 2701 *et seq*, (also referred to herein as the Electronics Communications Privacy Act or "ECPA".)

6. This Court has pendent jurisdiction of the related state law claims asserted in this complaint pursuant to 28 U.S.C. § 1367 because they arise from a common nucleus of operative facts related to and/or arising from Counts One and Two, and because the exercise of pendent jurisdiction serves the interests of judicial economy, convenience, and fairness to the parties.

7. Venue in this district is proper pursuant to 28 U.S.C. § 1391(b)(2) since some, or all, of the conduct which is the subject of this complaint occurred in Westchester County, New York.

COMMON ALLEGATIONS

8. Plaintiff and Defendant were married in November 2006 and have three minor children ("the Children"). In August 2010, Plaintiff filed an action for dissolution of marriage, which was withdrawn in September 2010. The parties then proceeded to reside together until May 2019, when Defendant filed a divorce action captioned, *Allan Kassenoff v. Catherine Kassenoff*, file no. 58217/2019, in the Supreme Court, Westchester County, New York ("the Divorce Action"). Defendant was and remains represented by Dimopoulos and the Firm in that proceeding.

9. The three-year period prior to the filing of the Divorce Action was contentious and marked with physical and emotional abuse by Defendant and repeated police involvement. In the months preceding the filing of the final Divorce Action, Defendant began making near-daily threats of divorce against Plaintiff. In February 2016, Defendant assaulted Plaintiff in their home, for which Plaintiff was treated at a nearby hospital. That same year, Defendant unilaterally declared an "open marriage."

10. Throughout the marriage, Plaintiff owned and utilized a number of electronic devices for personal and professional use. For portable communication, she used a periodically upgraded Apple iPhone to which number (917) 836-5200 was assigned. Additionally, Plaintiff utilized various features specific to Apple products such as Facetime, SMS text messaging and the Apple calling features that she transferred to each succeeding device she acquired. Plaintiff also incorporated other outside applications such as Google and Yahoo that enabled her to transmit and receive email messages via her hosted Gmail and Yahoo email accounts.[1]

11. In order to protect her iPhone from tampering or unauthorized access, Plaintiff activated and maintained the iPhone's passcode feature on each iPhone she used. The Apple iPhone passcode is a four-to-six-character user-selected numeric sequence that unlocks the device when it is turned on.

12. Throughout the marriage, Plaintiff did not share her iPhone passcode with anyone, including Defendant, nor did she permit Defendant to directly access her device.

13. At all relevant times, Plaintiff utilized Verizon Wireless for all her iPhone services, including text messaging, email, phone calls, Facetime and internet browsing services.

[1] Plaintiff's hosted email accounts addresses were ckassenoff@yahoo.com and clkassenoff@gmail.com.

Plaintiff was the primary account holder for her family's Verizon account through which Defendant used a shared family telephone plan; Defendant was a secondary user. Notwithstanding that one Verizon account was maintained for both parties, neither party had access to the other's iPhone passcode or credentials so as to enable access to the other party's communication applications.

14. At a point in time prior to 2016, Plaintiff and Defendant purchased a MacBook Pro laptop computer for their joint use ("the Laptop"). Each established separate user accounts that were separately password protected. Accordingly, each user could only access the data and applications established under each respective account. Although the Laptop was jointly accessible, Defendant subsequently used the Laptop far more frequently than did Plaintiff.

15. Apple products are designed to be interconnected such that applications and data accessible through one device can also be accessed from other connected Apple devices. In order to accomplish this, Apple requires that users obtain an Apple ID and password. Once this is obtained and activated, each device that has been integrated can access Apple services and all personal information and content associated with the account holder.

16. In 2016, Defendant stated that he wanted to purchase a particular song for his iTunes music library that he compiled on the Laptop. He asked Plaintiff for, and she provided, her Apple ID and Password to him for the express purpose of enabling him to make this purchase from the Apple iTunes Store. Defendant did not receive or obtain Plaintiff's authorization to use these credentials for any other purpose beyond this one-time purchase of music.

17. While in possession of Plaintiff's Apple ID and Password for this one time purchase, Defendant activated the "Find My iPhone" application on the Laptop with respect to

Plaintiff's iPhone. This application enables an individual to track the location of other connected Apple devices.

18. Plaintiff was not aware that Defendant had activated the Find My iPhone application on the Laptop.

19. Defendant continued to use Plaintiff's Apple ID and Password in other ways, including to "sync" Plaintiff's iPhone with the Laptop. Once synchronization between devices has initially occurred data can be subsequently directed by using access to the iCloud to automatically and remotely transfer files and data stored on the iCloud to interconnected devices.

20. After the syncing of Plaintiff's iPhone with the Laptop, Defendant accessed and intercepted Plaintiff's text message communications over the course of several years, an activity that Defendant has admitted to doing. Through such synchronization, Defendant received copies of Plaintiff's text messages at the same time Plaintiff received the message.

21. Plaintiff never authorized or consented to the use of her Apple ID and Password beyond the limited purpose of allowing Defendant to make a one-time purchase of a song on iTunes. At no time did Plaintiff agree to the "syncing" of her iPhone with the Laptop or with any other device. At no time did Plaintiff agree that Defendant (or anyone else) could access and intercept her private, confidential, and privileged text message communications, emails, or other data.

22. At all relevant times herein, Plaintiff considered her text messages and other electronic communications to be private and their contents confidential. Said communications included text and email messages with her attorney, Cynthia Monaco, Esq., an individual who Defendant, himself a lawyer, knew was a lawyer. Plaintiff also had numerous private and confidential communications by text message with family members, friends, and others.

23. The electronic communications Defendant accessed and intercepted from Plaintiff's iPhone included Plaintiff's private, confidential, and privileged electronic communications with various third parties, including her attorneys. Plaintiff did not know that Defendant had intercepted her electronic communications by using her iCloud account to synchronize the Laptop with her email and text message accounts.

24. Given that Defendant was receiving real-time incoming and outgoing text and email messages, including attorney-client electronic communications during the period of early 2016 to the filing of the Divorce Action in May 2019, Defendant had access to communications that discussed matrimonial litigation strategy, domestic abuse, and related issues and concerns.

25. Immediately upon the filing of the Divorce Action, the Firm, through Dimopoulos as Defendant's counsel, brought an *ex parte* Order to Show Cause in the Supreme Court of Westchester County which sought to exclude Plaintiff from the marital home and grant Defendant temporary custody of the Children.

26. Attached to Defendant's supporting papers were multiple screenshots of actual text messages transmitted by and between Plaintiff and Attorney Monaco discussing legal strategy. Defendant's affidavit included at least eleven text messages dated from September 2018 onward and several that were listed as "undated" ("the Text Messages").

27. This *ex parte* application was granted and Plaintiff was immediately removed from the marital home and Defendant was granted temporary sole legal and residential custody of the Children.

28. Plaintiff's opposition to the order to show cause was heard on June 7, 2019 at which time Plaintiff's counsel informed Dimopoulos that the text messages attached to the order

to show cause were privileged attorney-client communications that Defendant had obtained without having obtained Plaintiff's consent or authorization.

29. Despite Plaintiff's counsel's express warning that these electronic communications were privileged, confidential and private, Dimopoulos did not withdraw the Text Messages. Instead Dimopoulos continued to use and disclose these communications to additional individuals as the Divorce Action proceeded.

30. In the Summer of 2019, Defendants provided the Text Messages to Child Protective Services who was investigating Defendant for child abuse.

31. On or about September 6, 2019, Defendants again published the Text Messages in submissions to the court in the Divorce Action.

32. On or about October 7, 2019, Defendants provided the Text Messages to Dr. Marc Abrams, the court-appointed custody evaluator in the Divorce Action.

33. On or about March 16, 2020, Defendants again republished the Text Messages in a filing in the Divorce Action.

34. On or about March 25, 2020, and shortly after the COVID-19 pandemic was declared, Dr. Abrams, in reliance upon Text Messages provide to him by Defendant, recommended to the court that Plaintiff be excluded from her home and lose custody of the Children.

35. On or about March 27, 2020, Defendants obtained an *ex parte* order excluding Plaintiff from her home and granting temporary sole custody of the Children to Defendant; Plaintiff was rendered childless and homeless overnight.

36. It remains unclear how many private, confidential or privileged communications Defendant and Dimopoulos have accessed and/or intercepted, used or disclosed; Plaintiff is only

aware of those electronic communications that have been published and shared with the court and third parties associated with the Divorce Action on an ongoing and continuing basis. Accordingly, the full extent and timing of Defendant's and/or Dimopoulos' disclosure of Plaintiff's electronic communications is not known.

37. Defendant obtained Plaintiff's electronic communications either by intercepting them while they were transiting through her iCloud account or downloaded said communications while stored in Plaintiff's iCloud account, and in so doing violated provisions of the Electronic Communications Privacy Act. To the extent that Plaintiff's electronic communications were intercepted, as opposed to retrieved from storage at the internet service provider (ISP) level, Defendant, Dimopoulos and the Firm have also knowingly used and disclosed electronic communications protected by the Wiretap Act provisions of the Electronic Communications Privacy Act.

COUNT ONE
(Violation of 18 U.S.C. § 2511 – "The Wiretap Act")

38. Paragraphs 1 through 37 of this complaint are realleged and incorporated herein as if more fully set out.

39. At all relevant times herein, The Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.* was in full force and effect and governed the acquisition and disclosure of electronic communications, including the Text Messages, transmitted by electronic communications services.

40. At all relevant times herein, subject to specific exceptions, 18 U.S.C. § 2511 prohibited the intentional interception, or disclosure or use of the contents of any intercepted electronic communications obtained without the consent of at least one of the parties to that communication.

41. On information and belief, and commencing in 2016, Defendant intentionally intercepted Plaintiff's electronic communications, i.e. Text Messages and/or other communications, without her consent, by forwarding her communications to himself utilizing various Apple iCloud functions and features.

42. On diverse dates following Defendant's interception of Plaintiff's electronic communications, Defendant disclosed said communications and/or their contents to Dimopoulos, as well as to the Firm, and permitted their use and disclosure in court proceedings and pleadings.

43. On diverse dates following Defendant's interception of Plaintiff's electronic communications, Dimopoulos and the Firm re-disclosed said communications and/or their contents by using such communications in court proceedings and pleadings.

44. Upon information and belief, Dimopoulos knew, or had reason to know, that the information and documents disclosed to him by Defendant had been obtained through an interception of Plaintiff's electronic communications.

45. Upon information and belief, Dimopoulos knew, or had reason to know, that Defendant had intercepted Plaintiff's electronic communications without her consent, and that Plaintiff had not authorized the disclosure, re-disclosure, or use of such communications.

46. As a result of his management, decision-making, and control of the Firm, Dimopoulos' knowledge and actions with respect to the use and disclosure of Plaintiff's electronic communications is attributable to the Firm by virtue of this agency.

47. Defendant has violated 18 U.S.C. § 2511(1)(a), (c) and (d) by intercepting, using and disclosing Plaintiff's electronic communications.

48. Dimopoulos and the Firm have violated 18 U.S.C. § 2511(1)(c) and (d) by knowingly using and disclosing Plaintiff's electronic communications.

49. Pursuant to 18 U.S.C. § 2520, Plaintiff is entitled to relief for the Defendant's violations of 18 U.S.C. § 2511(1)(a), (c), and (d) and Dimopoulos' violations of 18 U.S.C. §§ 2511(1)(c) and (d).

COUNT TWO
(Violation of 18 U.S.C. § 2701 - Stored Communications Act)

50. Paragraphs 1 through 37 of this complaint are realleged and incorporated herein as if more fully set out.

51. At all relevant times herein, The Stored Communications Act, 18 U.S.C. § 2701 *et seq*. was in full force and effect and governed the accessing of facilities through which electronic communication service is provided.

52. At all relevant times herein, subject to specific exceptions, 18 U.S.C. § 2701(a) prohibited the intentional unauthorized accessing of a facility through which an electronic communication service is provided whereby an individual obtains access to an electronic communication which is in electronic storage in such system.

53. Upon information and belief, on diverse days between February 2016 and May 2019, Defendant violated 18 U.S.C. § 2701(a) by intentionally and repeatedly accessing Plaintiff's electronic communications while said communications were in electronic storage maintained by Apple, Google and/or Yahoo.

54. By intentionally accessing Plaintiff's electronic communications without authorization or by exceeding any authorization that may have been provided earlier, Defendant violated 18 U.S.C. § 2701(a) and is liable to Plaintiff for said violations.

COUNT THREE
(Trespass To Chattels)

55. Paragraphs 1 through 37 of this complaint are realleged and incorporated herein as if more fully set out.

56. At all relevant times herein, Plaintiff held a possessory interest in her electronic communications, including text messages and emails, the intrinsic value of which was based in part upon the confidential and private nature of the communications.

57. Through their actions, Defendant, Dimopoulos and the Firm intentionally intermeddled with Plaintiff's possessory interest in her electronic communications.

58. By intermeddling with Plaintiff's electronic communications, Defendant, Dimopoulos and the Firm dispossessed Plaintiff of the confidential and private aspects of said communications and used the information contained therein for their personal and professional gain thereby impairing the condition, quality, and value of Plaintiff's property.

59. By reason of the said trespass, Defendant, Dimopoulos and the Firm conducted themselves in a manner that was malicious, oppressive, outrageous, willful, wanton, reckless, and abusive thereby entitling Plaintiff to compensatory and punitive damages.

COUNT FOUR
(Prima Facie Tort - Violation of NY Penal Law Sec. 250)

60. Paragraphs 1 through 37 of this complaint are realleged and incorporated herein as if more fully set out.

61. Defendants had a statutory duty, pursuant to New York Penal Law § 250.05, to not commit electronic eavesdropping with respect to Plaintiff's electronic communications.

62. Defendant had an independent duty as Plaintiff's husband to not commit electronic eavesdropping with respect to Plaintiff's electronic communications.

63. Plaintiff is a user of electronic communications, and as such, is a member of the class for whom the protections of this statute were enacted.

64. The legislative purpose behind this statute, *i.e.*, the deterrence of illegal electronic eavesdropping, is enhanced and furthered through the private enforcement of tort remedies.

65. By reason of the conspiracy between the Defendant, Dimopoulos and the Firm, their commission of felonies by repeated violations of New York Penal Law § 250.05, and the aiding and abetting thereof, Defendants conducted themselves in a manner that was malicious, oppressive, outrageous, willful, wanton, reckless, and abusive so as to entitle Plaintiff to compensatory and punitive damages.

COUNT FIVE
(Temporary and Permanent Injunctive Relief Pursuant to 18 U.S.C. § 2520(b) and 18 U.S.C. § 2707(b))

66. Paragraphs 1 through 37 of this complaint are realleged and incorporated herein as if more fully set out.

67. As direct and proximate result of each Defendant's conduct as described herein, Plaintiff has suffered irreparable harm. Plaintiff has lost the confidentiality, privacy and privilege of her electronic communications.

68. Given that Plaintiff and Defendant are currently engaged in New York Supreme Court litigation, proceedings in which Dimopoulos represents Defendant, the Defendants' misappropriation, possession and continued use and disclosure of the confidential, private, and privileged information gained in violation of state and federal law poses a substantial risk of irreparable harm. The total loss to Plaintiff in economic terms cannot be accurately measured at this time.

69. Plaintiff has a substantial likelihood of success on the merits of her claims. In addition, the magnitude of the injury being suffered due to Defendants' unlawful conduct heavily outweighs whatever hardship each Defendant could allege or prove from being restrained as requested.

70. The granting of the injunctive relief requested herein will not adversely affect any public policy or public interest.

71. Injunctive relief, as an equitable remedy, is authorized by 18 U.S.C. § 2520(b) and 18 U.S.C. § 2707(b)), and as such Plaintiff need not demonstrate an irreparable injury or inadequacy of other remedies, but merely show a *prima facie* case of illegality and that an injunction would fulfill the legislative purpose of the statute. A temporary restraining order and preliminary injunction will fulfill the purposes of these statutes.

72. At this point, Plaintiff has no adequate remedy at law and is suffering immediate, imminent, and irreparable harm. Should Defendants' actions in using and disclosing the communications and information illegally obtained continue unabated, they will continue to harm Plaintiff's ability to proceed in Supreme Court as well impact her privacy interests.

73. Further, a substantial risk exists that in the absence of an appropriate order directing Defendants to preserve material evidence, Defendants will destroy or conceal evidence supporting the claims articulated in this Complaint. Specific items at risk of spoliation include, but are not limited to: digital storage devices; computer hard drives; files stored on-line; stored text message communications; downloaded text message communications and any attachments thereto; correspondence or memoranda summarizing the contents of Plaintiff's electronic communication or text messages; hard copies of Plaintiff's electronic communications; screen shots of Plaintiff's electronic communications; and photographs of Plaintiff's electronic

communications. Given that much of the evidence at issue is likely to be in digital format, the risk of loss through inadvertence, accident, or deliberate action is heightened. Should such evidence be lost, mishandled, or destroyed, Plaintiff's ability to establish her claims and damages will be threatened with irreparable harm.

74. There is reason to believe that in the absence of an immediate order restraining the destruction or manipulation of material evidence, such items will be destroyed or concealed. Defendant has consistently used his work email address - kassenoffa@gtlaw.com - to communicate with Defendant Dimopoulos, Plaintiff and others regarding the Text Messages and other communications.

75. Defendant has consistently used his work-issued computer and servers to download, store, create or modify documents relevant to the Text Messages and other communications.

76. Defendant continues to have exclusive access to, and use of a home desktop computer located in the marital residence that was purchased before the Divorce Action began. Upon information and belief, Defendant has used this computer to store information related to the Divorce Action, including the Text Messages and other communications.

77. Dimopoulos has used Dropbox, his law firm's on-line storage capabilities, and his law firm's computer systems to store, *inter alia*, to store, modify and create documents relevant to the illegally obtained Text Messages and other communications.

78. Issuance of a temporary restraining order requiring Defendants to preserve all material evidence in their possession, custody or control would aid in fulfilling the remedial purposes articulated in 18 U.S.C. § 2520(c) and 18 U.S.C. § 2707(c).

79. Plaintiff has not provided notice to Defendants of this action, or the relief sought herein on the grounds that to do so would accelerate the risk of destruction of evidence which Plaintiff is seeking to prevent. As to the requirement of a bond, the Court should set a minimum bond amount of no more than $100.00 on the grounds that the relief being sought will not cause damage to Defendants in that Defendants have no legal right to possess, disclose or use Plaintiff's Electronic Communications or any derivative materials.

80. Accordingly, Plaintiff requests a temporary restraining order and temporary and permanent injunctions against Defendants, their agents, servants, employees and those persons in active concert or participation with them, from:

(a) Deleting, altering, destroying or removing any electronic communications directly or indirectly originating from Plaintiff's e-mail accounts, i.e. ckassenoff@yahoo.com and clkassenoff@gmail.com, or Text Messages;

(b) Deleting, altering, destroying or removing any hard copy of any electronic communications or attachments thereto which directly or indirectly originated from Plaintiff's e-mail accounts, i.e. ckassenoff@yahoo.com and clkassenoff@gmail.com, or Text Messages;

(c) Deleting, altering, destroying or removing any summary of any e-mails or electronic communications or attachments thereto which directly or indirectly originated from Plaintiff's e-mail accounts, i.e. ckassenoff@yahoo.com and clkassenoff@gmail.com, or Text Messages;

(d) Directly or indirectly using or disclosing any information contained within any of Plaintiff's electronic communications or documents attached to any such electronic communications that Defendants may have received which

directly or indirectly originated from Plaintiff's e-mail accounts, i.e. ckassenoff@yahoo.com and clkassenoff@gmail.com, or Text Messages;

81. Plaintiff further requests that the Court enter Temporary Restraining Orders requiring:

(a) Defendants to preserve all evidence of any disclosure or dissemination of Plaintiff's electronic communications or any information contained therein;

(b) Defendants to preserve any and all portable or fixed electronic storage devices, including but not limited to, hard drives, floppy disks, on-line storage, thumb or zip drives, compact disks or flash drives, which may contain Text Messages or electronic communications directly or indirectly originating from Plaintiff's e-mail accounts, i.e. ckassenoff@yahoo.com and clkassenoff@gmail.com, or Text Messages; or which may contain any summaries of information derived from Plaintiff's e-mail accounts, i.e. ckassenoff@yahoo.com and clkassenoff@gmail.com, or Text Messages; or which may contain evidence of any disclosure or dissemination of Plaintiff's electronic communications or any information contained therein;

(c) that pending further order of this Court, all items and materials covered by this order shall be preserved in such a manner as to maintain the integrity of the data, including all associated meta-data existing as of the date of this order;

(d) that the Court, pursuant Fed. R. Civ. P. 53, appoint a Special Master with training or knowledge in computer forensics to examine all electronic storage devices and media in the possession, custody or control of Defendants, to the extent that such items were used to store data related to any interception of Plaintiff's electronic communications or e-mail at any time prior to the date of service of this Order, for the purpose of identifying any electronic communications or data material to this action, and to perform any other function or duty ordered by the Court. Defendants will incur the expenses to have each such item imaged for the purposes of preserving, cataloging and subject to further order, locating evidence.

82. The Temporary Restraining Order, as requested above, is warranted in that it would be of assistance in preserving the status quo.

WHEREFORE, Plaintiff requests a trial by jury and that judgment enter against Defendants as follows:

1. Compensatory damages;

2. Statutory damages pursuant to 18 U.S.C. § 2520(c) and 18 U.S.C. § 2707(c);

3. Punitive damages pursuant to 18 U.S.C. § 2520(b) and 18 U.S.C. § 2707(c) and the common law;

4. Attorney's fees and costs pursuant to 18 U.S.C. § 2520(b) and 18 U.S.C. § 2707(b);

5. A temporary and permanent order, pursuant to 18 U.S.C. § 2520(b) and 18 U.S.C. § 2707(b), directing Defendants to return to Plaintiff all copies of all electronic communications, whether stored in an electronic format or printed;

6. A temporary and permanent order, pursuant to 18 U.S.C. § 2520(b) and 18 U.S.C. § 2707(b), barring Defendants from disclosing the contents of any electronic communications obtained in violation of federal law.

7. A temporary and permanent order, pursuant to 18 U.S.C. § 2520(b) and 18 U.S.C. § 2707(b), directing Defendants to cease and desist from engaging in any electronic monitoring, surveillance or wiretapping of Plaintiff;

8. A temporary restraining order issue pursuant to 18 U.S.C. § 2520(b) and 18 U.S.C. § 2707(b), ordering the Defendants to preserve all documentary and physical evidence in their care, custody, or control, including all electronic devices that may contain any evidence of Plaintiff's electronic communications;

9. Such further and additional relief as this Court may find to be fair and equitable.

CATHERINE KASSENOFF

By _____

Harold R. Burke (HB0149)
Law Offices of Harold R. Burke
P.O. Box 4078
Greenwich, CT 06830
Telephone: (203) 219-2301
Facsimile: (203) 413-4443
E-Mail: hrb@burke-legal.com