IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CORY HUBBARD, individually, and on behalf of a class of all others similarly situated, **Plaintiff,** **v.** **MYSPACE, INC.,** **Defendant.**	**Index No.: 11-cv-00433 (LAK)** **ECF CASE**

MEMORANDUM OF LAW IN RESPONSE AND OPPOSITION TO MYSPACE, INC.'S MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

I. INTRODUCTION 1

II. STATEMENT OF FACTS 3

A. Procedural History 3

B. Facts Supporting Plaintiff's Claims 3

III. ARGUMENT 8

A. Standard of Review 8

B. The SCA Protects Important Privacy Interests 8

C. The SCA Has Two Defenses: Valid Compulsory Process and Good Faith Reliance On Invalid Compulsory Process, Neither of Which Are Available to MySpace 12

1. 18 U.S.C. § 2703(e) Requires That Disclosure be Pursuant to a Warrant Issued in Accordance with the SCA *i.e.*, by a "Court of Competent Jurisdiction" 13

2. The Warrant Was Not Issued by a Court of Competent Jurisdiction 14

a. A Georgia Magistrate Court is *Not* a Court of General Criminal Jurisdiction and Therefore *Not* a Court of Competent Jurisdiction as Defined in the SCA 15

b. MySpace Ignores the Plain Language of 18 U.S.C. § 2711(3)(B), Relying Instead on Unrelated, Distinguishable Cases 15

c. A Georgia Magistrate Court Cannot Issue a Search Warrant for a Search of Property Outside its County 17

3. 18 U.S.C. § 2707(e) Requires Objective Reasonableness, *i.e.*, A Facially Valid Warrant 17

D. Although the Practice of Law Enforcement Faxing Out of State Warrants to Providers is Widespread, It Still Violates the SCA 20

IV. CONCLUSION 23

TABLE OF AUTHORITIES

Cases **Page**

Ashcroft v. Iqbal, --U.S.--,
129 S. Ct. 1937 (2009) 8

Bansal v. Microsoft Hotmail,
267 Fed. Appx. 184 (3d Cir. 2008).....19

Bansal v. Server Beach,
285 Fed. Appx. 890 (3d Cir. 2008) 18-19

Beck v. State,
283 Ga. 352, 658 S.E.2d 577 (Ga. 2008) 17

Bell Atl. Corp. v. Twombly,
550 U.S. 554 (2007) 8

Crispin v. Christian Audigier, Inc.,
717 F. Supp. 2d 965 (C.D. Cal. 2010) 12

Edgar v. Mite Corp.,
457 U.S. 624, 631 (1982) 14

Freedman v. Am. Online, Inc.,
325 F. Supp. 2d 638 (E.D. Va. 2004) 12, 17, 18, 20

Harris v. Mills,
572 F.3d 66 (2d Cir. 2009) 8

In re Application by the United States of Am. for a Search Warrant,
665 F. Supp. 2d 1210 (D. Or. 2009) 21

In re Search of Yahoo, Inc.,
2007 WL 1539971 (D. Ariz. May 21, 2007) 21

In re Search Warrant,
2005 WL 3844032 (M.D. Fla. Dec. 23, 2005).....21

Ins. Corp of Ireland, Ltd. v. Compagnie des Bauxites de Guinee,
456 U.S. 694 (1982) 16

Jayne v. Sprint PCS,
2009 WL 426117 (E.D. Cal. Mar. 26, 2009) 19

McReady v. eBay, Inc.,
453 F.3d 882 (7th Cir. 2006) 19

Post Dock & Stone Corp. v. Oldcastle Ne., Inc.,
507 F.3d 117 (2d Cir. 2007) 8

Quon v. Arch Wireless Operating Co., Inc.,
529 F.3d 892 (9th Cir. 2008) 9

Silverthorne Lumber Co. v. United States,
251 U.S. 385 (1920) 9

Sinoying Logistics Pte Ltd. v. Yi Da Zin Trading Corp.,
619 F.3d 207 (2d Cir. 2010) 16

State v. Kelley,
302 Ga. App. 850, 691 S.E.2d 890 (Ga. Ct. App. 2010) 17

State v. Lejeune,
277 Ga. 749, 594 S.E.2d 637 (Ga. 2004) 15, 17

Stone v. City & County of San Francisco,
968 F.2d 850, 862 (9th Cir. 1992),
cert. denied, 113 S. Ct. 1050 (1993) 14

Storey v. Cello Holdings, L.L.C.,
347 F.3d 370 (2nd Cir. 2003) 16

United States v. Berkos,
543 F.3d 392 (7th Cir. 2008) 21

United States v. Councilman,
418 F.3d 67 (1st Cir. 2005) 12

United States v. Kernell,
2010 WL 1408437 (E.D. Tenn. Apr. 2, 2010) 21

United States v. Morton,
467 U.S. 822 (1984) 16

FEDERAL STATUTES

18 U.S.C. § 2232 8

18 U.S.C. § 2701.....2

18 U.S.C. § 2702 .....10, 13

18 U.S.C. § 2702(c)(4) 19

18 U.S.C. § 2703 .....10, 11, 13, 15, 20

18 U.S.C. § 2703(d) 10

18 U.S.C. § 2703(e) 13, 14, 19

18 U.S.C. § 2703(g) 20

18 U.S.C. § 2707(e) ..... passim

18 U.S.C. § 2708 2

18 U.S.C. § 2711(3)(B) 14, 15, 16

28 U.S.C. § 1915(e) 19

Fed. R. Civ. P. 5.2 3

Fed. R. Civ. P. 15(a)(1)(b) 3

Fed. R. Crim. P. 41 21

STATE STATUTES

Cal. Penal Code § 1524.2(c) 22

Cal. Penal Code § 1524.2(d) 23

Ga. Const. art. VI, § III, para. I 15

Ga. Const. art. VI, § IV, para. I 15

O.C.G.A. § 15-10-2 15

O.C.G.A. § 15-6-8 15

Mass. Gen. Laws Ann. ch. 276 § 1B(d).....22

Va. Code Ann. § 19.2-70.3 22

MISCELLANEOUS

Nathaniel Gleicher, *Neither a Customer nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 9

Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569 (2007) 9

U.S. Internet Serv. Provider Ass'n, *Electronic Evidence Compliance – A Guide for Internet Service Providers*, 18 BERKELEY TECH. L.J. 945 (2003).....9

Plaintiff Cory Hubbard ("Plaintiff"), through his undersigned counsel of record, respectfully submits this Memorandum of Law in Response and Opposition to MySpace, Inc.'s Motion to Dismiss and in support thereof sets forth as follows:

I. INTRODUCTION

In its Motion to Dismiss, Defendant MySpace, Inc. ("MySpace" or "Defendant") elected to follow the old legal adage, "When the law is against you, argue the facts. When the facts are against you, argue the law. When both are against you, attack the plaintiff." It is with this brazen and pompous legal strategy that MySpace attacks Plaintiff and baselessly, indeed frivolously, threatens Rule 11 sanctions in an attempt to shift this Court's attention from the actual issues. Despite the ample factual and legal basis for this lawsuit, and, significantly, MySpace's own concession that this case presents issues of first impression (Def. Mem. at 17)[1], Defendant nonetheless levels a request for sanctions in an effort to scare off Plaintiff.[2]

Notably, MySpace ignores its very own publicized statements that while it would prefer to give law enforcement the information it seeks without being compelled to do so, the Electronic Communications Privacy Act of 1986 (the "ECPA") and each state's laws prohibit such information from being shared without proper legal process. (AC, ¶¶ 14 – 22).[3] In fact, as alleged in the Amended Complaint, MySpace claims that every time a request comes in, it must ensure that it jumps through the precise legal hoops to fully comply with each state's laws and

---

[1] Page references to the Memorandum of Law in Support of MySpace, Inc.'s Motion to Dismiss the Class Action Complaint are cited as "Def. Mem. at __."

[2] Should the Defendant make good on its threat, Plaintiff intends to respond in kind. Indeed, the Advisory Committee Notes observe that the filing of a frivolous Rule 11 motion "is itself subject to the requirements of the rule and can lead to sanctions."

[3] Paragraph references to Plaintiff's Amended Class Action Complaint are cited as "AC, ¶__."

process. However, as alleged in the Amended Complaint, it is precisely these precautionary steps that MySpace flouts.

MySpace also spends a considerable amount of time personally attacking Plaintiff in an attempt to poison the proverbial well. Yes, Plaintiff is admittedly a convicted sex offender. However, neither Plaintiff's conduct nor his guilty plea is in any way relevant to any question presently before this Court. While Plaintiff's criminal history may render him an unsympathetic individual, Mr. Hubbard nevertheless has rights afforded by federal and state law, the same as any other person. It is thus ironic that a Defense team, led by a respected former jurist and public servant, is advancing an argument that the law should not be applied evenhandedly to both innocent and guilty alike.

As much as MySpace would like to convince this Court that the Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA"), infers an "unlikeable plaintiff" defense -- it does not, even in the most extreme cases.[4] Plaintiff, like any other person entitled to the protections afforded by the SCA, is well within his rights to bring this action, irrespective of whether MySpace respects him as a person. Moreover, Plaintiff brings this action on behalf of a class -- a class full of individuals who were merely visitors, members, subscribers, customers or users of MySpace services ("MySpace Users"), and who were never convicted or even accused of illegal conduct, but whose privacy rights were violated nevertheless.[5]

---

[4] Nor, for that matter, does the SCA contain an exclusionary rule from use in a criminal case any information produced in violation of its terms. The remedies and sanctions described in the SCA are the only judicial remedies and sanctions for nonconstitutional violations of the SCA. 18 U.S.C. § 2708. In other words, Defendant's only incentive not to violate the non-disclosure provisions of the SCA is to avoid actions such as this lawsuit.

[5] Defendant's lack of concern for the privacy of third parties is not limited to Plaintiff. In its rush to attack the Plaintiff, Defendant twice filed documents containing the names and home addresses of every witness in the criminal case, *including the minor* at issue, who is identified by her full name and home address. (Declaration in Support of Motion to Dismiss Complaint, pp.

The straightforward (and relevant) facts of this case show that MySpace impermissibly disclosed Mr. Hubbard's personal and private user information, data, records and the contents of electronic communications to law enforcement in response to a warrant that was invalid on its face. Because MySpace did so without Mr. Hubbard's knowledge or authorization, and without valid and enforceable legal process, it violated the SCA. In addition to ignoring the plain language of the statue, Defendants have not put forth a single legal authority that belies Plaintiff's well-grounded claim. Accordingly, Defendant's Motion should be denied.

II. STATEMENT OF FACTS

A. Procedural History

This case was initially filed on January 20, 2011, in the United States District Court, Southern District of New York. Defendant filed a Motion to Dismiss and Memorandum of Law in Support Thereof on February 11, 2011. After reviewing the arguments raised in Defendant's initial Motion to Dismiss, Plaintiff reevaluated and narrowed his claims and timely filed on February 25, 2011, the Amended Complaint as a matter of right pursuant to Fed. R. Civ. P. 15(a)(1)(b). On March 2, 2011, Defendant filed its second Motion to Dismiss and Memorandum of Law in Support Thereof.

B. Facts Supporting Plaintiff's Claims

The following factual assertions are drawn from the Amended Complaint filed by Plaintiff. (AC, ¶¶ 1 – 39). These are the facts which must be deemed to be true for purposes of Defendant's Motion to Dismiss.

28-32 and 90; Declaration in Support of Motion to Dismiss Amended Complaint, pp. 28-32 and 90). Defendant thereby violated Fed. R .Civ. P. 5.2, the E-Government Act of 2002, and Section 21.3 of the Southern District of New York Electronic Case Filing Rules and Instructions.

This is a class action lawsuit against MySpace for improperly, voluntarily, and knowingly disclosing certain personal and private user information, data, records and/or the contents of electronic communications in violation of the privacy rights of MySpace Users. MySpace disclosed personal and private user information, data, records and the contents of electronic communications of MySpace Users to law enforcement and other government entities without the MySpace Users' knowledge or authorization and without valid and enforceable legal process. The impermissibly disclosed personal and private user information, data, records and the contents of electronic communications included, but was not limited to, some or all of the following: full name, mailing address, telephone number, credit card number, gender, relationships, date account created, account status, email address, the content of email communications, content of private messages in the MySpace User's Inbox and sent mail folders, contact lists, photos, videos, files, website posts, registration from Internet Protocol (IP), date IP registered, IP address at account sign-up, login IP addresses, logs showing IP address and date stamps for account accesses, and other IP address information.

Plaintiff is a resident of the state of Georgia and a MySpace User. On or about February 11, 2008, Plaintiff had his personal and private user information, data, records and/or the contents of electronic communications disclosed by MySpace to law enforcement and other government entities without proper compliance with the compelled disclosure provisions of the SCA. The SCA was enacted in 1986 as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), and sets forth a system of statutory privacy rights for customers, users and subscribers of internet businesses, consumer services and computer network service providers such as MySpace.

MySpace operates http://www.myspace.com, which is a social networking platform that allows members to create unique personal profiles in order to find and communicate with old and new friends. MySpace is part of News Corp.'s Digital Media Group, f/n/a Fox Interactive Media, which in public filings reported that MySpace had nearly 70 million unique users in the United States and approximately 101 million unique users worldwide. In its Terms of Use Agreement and MySpace Privacy Policy, MySpace claims it protects MySpace Users' privacy as required by law and applicable privacy policies. MySpace hired Hemanshu Nigam as it Chief Security Officer in 2006, and in May 2007, MySpace refused to comply with a letter request from the attorney generals of eight states to hand over the names of registered sex offenders who used the MySpace social networking website because MySpace indicated that proper legal process was not followed. In an Associated Press interview (AC, Ex. A), MySpace's Chief Security Officer, Hemanshu Nigam, said: "We're truly disheartened that the AGs chose to send out a letter … when there was an existing legal process that could have been followed."

Shortly thereafter, on or about May 21, 2007, MySpace unveiled a plan for cooperating with state law enforcement for the disclosure of personal and private information and data of MySpace Users. MySpace had acknowledged that it could not turn over the information under the terms of the ECPA and it agreed the ECPA, as well as some state privacy laws, prohibited such information from being shared without a subpoena.

In a CNET News article (AC, Ex. B), Michael Angus, then the Executive Vice President and General Counsel of Fox Interactive Media (a parent company of MySpace) said, "It's simply a matter of making sure we jump through the right legal hoops … The process is really just compliance with each of the state laws, so each state has their own process that they have to follow" when speaking about MySpace's plan for cooperation. In an interview with Reuters,

(AC, Ex. C), Mr. Angus gave further detail about MySpace's plan to cooperate with law enforcement and stated, "Each state has its own laws… *It's an intricate web of laws that we make sure we comply with* …" (Emphasis added).

In a February 4, 2009, letter to the Honorable Roy Cooper, Attorney General of North Carolina, (AC, Ex. D), Mr. Angus provided an update on MySpace's assistance with law enforcement and clarified that federal law *requires* that a subpoena be issued before they can produce the requested information to law enforcement. Specifically, Mr. Angus, on behalf of MySpace, stated: "MySpace does not hide or withhold this information as some suggest. We would prefer to give it to law enforcement without a subpoena, but federal law does not permit this. No law enforcer needs to "compel" MySpace to produce this data – we want to give it to you." Recognizing the importance of the privacy rights of MySpace Users, in an interview with CNET in February 2010, (AC, Ex. E), Mr. Nigam on behalf of MySpace further acknowledged, "You can be very supportive of law enforcement investigation and at the same time be very cognizant and supportive of the privacy rights of our users." Mr. Nigam claimed, "Every time a legal process comes in, whether it's a subpoena or a search order, we do a legal review to make sure it's appropriate." In a March 2010, interview, (AC, Ex. F), Mr. Nigam said that MySpace "want[s] to make sure that our users' privacy is protected and any data that's disclosed is done under proper legal process."

MySpace appeared to pride itself publicly on strict compliance with legal process – so much so that it set up a unit to comply with the myriad state and federal laws. Perhaps these statements were nothing more than sound bites for the media and its already dwindling membership base meant to reassure that MySpace was acting in accordance with the applicable laws. Whatever the case, the fact is MySpace routinely and unlawfully accepts invalid legal

process from law enforcement and other government entities, such as in the case of the Plaintiff where it accepted a facsimile transmission in California of an out-of-state search warrant signed by a county magistrate judge in Georgia who was without authority to issue such a warrant.

Neither state search warrants signed by magistrates and other state judges nor state grand jury or trial subpoenas have any force and effect outside the limits of that state courts' territorial jurisdiction, and when faxed or sent out of that state, are facially invalid, unenforceable and not issued by a court of competent jurisdiction. MySpace's disclosure of a MySpace User's personal and private user information, data, records and/or the contents of electronic communications in response to facially invalid and unenforceable foreign state warrants, foreign state grand jury or trial subpoenas or voluntarily in response to letter requests, is improper and violative of federal and state law.

What MySpace did in this case is typical of its normal and routine business practice. On January 29, 2008, Sergeant Chris Haffner of the Cherokee County, Georgia Sheriff's Office faxed a state search warrant signed by a Judge of the Magistrate Court of Cherokee County, Georgia to the Custodian of Records of MySpace.com in Beverly Hills, California. The state search warrant was facially invalid and unenforceable as it: (a) was not properly served on MySpace; (b) purported to authorize a search by law enforcement of property beyond the jurisdictional limits afforded to a Cherokee County Magistrate; (c) purported to authorize a search by law enforcement of a witness beyond the jurisdictional limits afforded to a Cherokee County Magistrate; (d) purported to authorize a seizure by law enforcement of property beyond the jurisdictional limits afforded to a Cherokee County Magistrate; and (e) purported to require and compel a response from the Custodian of Records of MySpace.com, a witness beyond the jurisdictional limits afforded to a Cherokee County Magistrate. On February 11, 2008, in

violation of the SCA, MySpace voluntarily accessed, produced and disclosed the requested personal and private user information, data, records and the contents of electronic communications to law enforcement, notwithstanding MySpace's actual knowledge that the state search warrant was invalid and unenforceable.

III. ARGUMENT

A. Standard of Review

On a motion to dismiss, the Court considers the legal sufficiency of the complaint, "taking its factual allegations to be true and drawing all reasonable inferences in the plaintiff's favor." *Harris v. Mills*, 572 F.3d 66, 71 (2d Cir. 2009) (citing *City of New York v. Beretta U.S.A. Corp.*, 524 F.3d 384, 392 (2d Cir. 2008)). Drawing all inferences in plaintiff's favor, the Court then determines whether the claim to relief "is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 554, 570 (2007). Facial plausibility is established when a plaintiff's allegations are not mere conclusory statements, but contain "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, --U.S.--, 129 S. Ct. 1937, 1949 (2009) (citing *Twombly*, 550 U.S. at 556). Where, as here, the factual allegations "actively and plausibly suggest" a claim, the motion to dismiss should be denied. *Post Dock & Stone Corp. v. Oldcastle Ne., Inc.*, 507 F.3d 117, 121 (2d Cir. 2007).

B. The SCA Protects Important Privacy Interests

Congress passed the SCA as part of the ECPA.[6] "The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment

[6] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2232, 2510–21, 2701–11, 3117 and 3121–26 (2000 & Supp. 2003)). *See generally* U.S. Internet Serv. Provider Ass'n, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 BERKELEY TECH. L.J. 945 (2003)

does not address." *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008) (citing Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209-13 (2004)).[7] Its creation was necessary because "two established lines of Fourth Amendment doctrine . . . strongly suggested that if the Constitution was the sole source of protection for remotely-stored electronic communications, then third parties, including the government, would face no obstacle to compelling disclosure." *See* Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 574 (2007). Accordingly, the ECPA embodies Congress' belief that new federal statutes were necessary to ensure that privacy interests in new forms of electronic communication were protected by well established constitutional standards. *Id.* at 573.

As Justice Holmes stated deftly in *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920), a line must be drawn somewhere to prevent the Fourth Amendment's guarantee against unreasonable searches and seizures from becoming no more than a "form of words." As it relates to that same premise, the SCA is meant to bridge the gap between the Fourth Amendment's more general prohibition on illegal search and seizure and the unforeseen privacy concerns borne by the Internet age. It is intended to prevent providers of remote computing services or electronic communication services ("Providers"), like MySpace, from divulging

---

(providing "general guidelines for Internet service provider compliance with law enforcement and national security evidence gathering authorities.").

[7] *See also* Nathaniel Gleicher, *Neither a Customer nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1945 (2009) ("Although the SCA was not intended to be 'a catch-all statute designed to protect the privacy of stored Internet communications,' it has been pressed into this role. Without the SCA to balance the interests of users, law enforcement, and private industry, communications will be subjected to a tug-of-war between the private companies that transmit them and the government agencies

private communications to certain entities and individuals. *Kerr*, *supra*, at 1213. The SCA "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." *Id.* at 1212.

In filling the gap, Congress sought to "ensure the continued vitality of the Fourth Amendment" and prevent the "gradual erosion" of privacy rights, but equally to avoid a situation where "[t]he lack of clear standards may expose law enforcement officers to liability and may endanger the admissibility of evidence." *Id.* The statute's framework thus reflects the twin goals of constraining private ISPs from vitiating privacy interests through voluntary disclosures, and ensuring that these constraints also provide a clear mechanism for law enforcement to compel disclosure in appropriate circumstances and keep it within appropriate procedural safeguards.

First, the SCA prohibits voluntary disclosure of information about customers and subscribers to any third party, including law enforcement. 18 U.S.C. § 2702. This prohibition ensures that Providers cannot, *via* a private search and voluntary disclosure, circumvent the Fourth Amendment. Second, the SCA imposes a series of "exceptions" to this prohibition that limits the government's right to compel Providers to disclose information in their possession about their customers and subscribers and only permits disclosure to law enforcement pursuant to specified legal process. 18 U.S.C. § 2703. "Although the Fourth Amendment may require no more than a subpoena to obtain e-mails, the statute confers greater privacy protection." *Kerr*, *supra*, at pp. 1212-13.

To protect the array of privacy interests of customers and subscribers, the SCA offers varying degrees of legal protection depending on the perceived importance of the privacy interest

---

that seek to access them. Internet users will find themselves with little protection," *quoting Kerr*,

involved. Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not. Law enforcement and the providers must apply the various classifications set forth in the SCA to the facts of each case to figure out the proper procedure for obtaining the information sought.

The SCA, more particularly § 2703, articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including email and voice mail) and other information such as account records and basic subscriber and session information. It provides five mechanisms that a "government entity" can use to compel a provider to disclose certain kinds of information. The five mechanisms are as follows: (1) subpoena; (2) subpoena with prior notice to the subscriber or customer; (3) § 2703(d) court order; (4) § 2703(d) court order with prior notice to the subscriber or customer; and (5) search warrant.

One feature of the compelled disclosure provisions of the SCA is that greater process generally includes access to information that cannot be obtained with lesser process. Thus, a 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a 2703(d) order can compel (and then some). As a result, law enforcement and providers are restricted by the procedural safeguards of the SCA with respect to what is a permissible disclosure.

---

supra, at 1214 (footnote omitted)).

C. The SCA Has Two Defenses: Valid Compulsory Process and Good Faith Reliance On Invalid Compulsory Process, Neither of Which Are Available to MySpace

The SCA provides two affirmative defenses to liability -- neither of which affords protection for MySpace in this matter. First, the SCA, specifically 18 U.S.C. § 2703(e), requires the Defendant to show that it "provid(ed) information, facilities, or assistance ***in accordance with the terms of*** a court order, warrant, subpoena, statutory authorization, or certification ***under this chapter*** [18 U.S.C. § 2701, et seq.]" *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 974 (C.D. Cal. 2010) (emphasis added). Alternatively, 18 U.S.C. § 2707(e) permits a Defendant to invoke a "good faith" defense, containing both a subjective component and an objective component. *Freedman v. Am. Online, Inc.*, 325 F. Supp. 2d 638 (E.D. Va. 2004) (citing *Jacobson v Rose*, 592 F.2d 515, 522-24 (9th Cir 1978)). The "good faith" defense requires Defendant to show that it both believed it was acting pursuant to a valid warrant and that its belief was reasonable based on the specific circumstances (*i.e.*, the information available to defendant concerning the legality of the process). *Freedman*, 325 F. Supp. 2d at 648.

Defendant argues, wrongly, that the validity or facial invalidity of the warrant is irrelevant because the SCA "immunizes" it from liability for the disclosures in this case. *See, e.g.* Def. Mem. at 13. However, the word "immunity" appears nowhere in the SCA and its use represents a blatant mischaracterization of the statute by MySpace.[8] To the contrary, both 18 U.S.C. § 2703(e) and 18 U.S.C. § 2707(e) are fact-based affirmative defenses, which Defendant bears the burden of proving. *United States v. Councilman*, 418 F.3d 67, 83 (1st Cir. 2005) ("We may neither expand the good faith defense's scope, nor convert it from a fact-based affirmative

[8] Despite chastising Plaintiff for paraphrasing a statute (Def. Mem. at 8-9), neither the word immunity nor any derivation thereof appears anywhere in the text of the SCA as MySpace would lead this Court to believe.

defense to a basis for dismissing an indictment on legal grounds."). Considering the great lengths MySpace has gone to portray itself as a zealous adherent to federal and state laws, there is certainly a factual determination to be made as to how much MySpace knew when it accepted a facially invalid search warrant from a county magistrate in Georgia. Consequently, Defendant has not and cannot meet that burden here, and its Motion to Dismiss should be denied.

1. 18 U.S.C. § 2703(e) Requires That Disclosure be Pursuant to a Warrant Issued in Accordance with the SCA *i.e.*, by a "Court of Competent Jurisdiction"

As set forth *supra*, the SCA prohibits the Defendant from voluntarily disclosing information about MySpace Users to any third party, including law enforcement. 18 U.S.C. § 2702. Under the SCA, Defendant may only provide information protected from disclosure by the SCA in response to certain specified legal process. 18 U.S.C. § 2703. As relevant to the facts of this matter, 18 U.S.C. § 2703 permits disclosure "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by ***a court of competent jurisdiction.***" (emphasis added).

18 U.S.C. § 2703(e) provides a defense to a cause of action against Providers disclosing information under the SCA where the disclosure is "***in accordance with the terms of*** a court order, warrant, subpoena, statutory authorization, or certification ***under this chapter***." A "warrant … under this chapter" is a warrant "issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." Thus, (as it relates to warrants) 18 U.S.C. § 2703(e) only provides a defense to a cause of action against Providers disclosing information in accordance with the terms of a warrant issued using the procedures described in the Federal

Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.

2. The Warrant Was Not Issued by a Court of Competent Jurisdiction

In an attempt to create its own self-serving definition of a "court of competent jurisdiction," MySpace ignores entirely the statutory definition as ***specifically set forth in the SCA***, and instead relies on a series of unrelated, distinguishable cases. While chastising Plaintiff for paraphrasing a statute, Defendant fails to even cite the statutory definition of a "court of competent jurisdiction" (as it relates to State courts), which is specifically contained and defined in the SCA. As used in the SCA, a "court of competent jurisdiction" is "a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants…" 18 U.S.C. § 2711(3)(B).[9] This does not describe the county magistrate court which issued the warrant here.

[9] The SCA, being a federal law and containing its own requirements regarding what is a proper warrant or a "court of competent jurisdiction" would, under the supremacy clause, override California, Virginia, Minnesota or any other state law purporting to establish a different standard. U.S. Const. art. VI, Paragraph 2 ("This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the contrary notwithstanding."). Under the Supremacy Clause, everyone must follow federal law in the face of conflicting state law. It has long been established that "a state statute is void to the extent that it actually conflicts with a valid federal statute" and that a conflict will be found either where compliance with both federal and state law is impossible or where the state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress. *Edgar v. Mite Corp.*, 457 U.S. 624, 631 (1982). Similarly, "otherwise valid state laws or court orders cannot stand in the way of a federal court's remedial scheme if the action is essential to enforce the scheme." *Stone v. City & County of San Francisco*, 968 F.2d 850, 862 (9th Cir. 1992), *cert. denied*, 113 S. Ct. 1050 (1993).

a. A Georgia Magistrate Court is *Not* a Court of General Criminal Jurisdiction and Therefore *Not* a Court of Competent Jurisdiction as Defined in the SCA

The Cherokee County, Georgia Magistrate Court that issued the warrant for Plaintiff was neither a court of "general criminal jurisdiction" *nor* authorized by Georgia law to issue a warrant for a search outside of Cherokee County, Georgia. In Georgia, a Magistrate Court is a court of limited jurisdiction. *See* Ga. Const. art. VI, § III, para. I; O.C.G.A. § 15-10-2. In contrast, in Georgia, the Court of general criminal jurisdiction is the Superior Court. *See* O.C.G.A. § 15-6-8. Ga. Const. art. VI, § IV, para. I; *State v. Lejeune*, 277 Ga. 749, 594 S.E.2d 637 (Ga. 2004). Thus, a Georgia Magistrate Court is not "a court of general criminal jurisdiction" and, therefore, is not a "court of competent jurisdiction" as defined under the SCA. As a result, the warrant upon which Defendant relies was unmistakably facially invalid, as it is apparent from the warrant's face that it was issued by a county magistrate court in Georgia and not issued by a court of competent jurisdiction.

b. MySpace Ignores the Plain Language of 18 U.S.C. § 2711(3)(B), Relying Instead on Unrelated, Distinguishable Cases

Instead of acknowledging the plain meaning of a "court of competent jurisdiction" as set forth in 18 U.S.C. § 2711(3)(B), MySpace attempts to mislead the Court by engaging in red herring arguments. 18 U.S.C. § 2703 clearly states that MySpace could only disclose privacy information based upon a search warrant issued by a court of competent jurisdiction. Since the Cherokee County, Georgia Magistrate Court is clearly not a "court of competent jurisdiction," as specifically defined by the SCA, MySpace attempts to deflect this Court from focusing on the express terms of the statute by urging the Court to rely instead on a judicially crafted definition fashioned by courts acting in the absence of a statute specifically defining the term.

MySpace submitted four cases in its deflection attempts. For example, in *United States v. Morton*, 467 U.S. 822 (1984), arising from a dispute about whether the underlying garnishment was issued by a court of competent jurisdiction, the Supreme Court found that the statute did not explicitly define "court of competent jurisdiction," unlike the instant case, and thus, the Court was left to decipher the meaning from the remainder of the statute. Defendant's reliance on *Storey v. Cello Holdings, L.L.C.*, 347 F.3d 370 (2nd Cir. 2003) is also misguided. In *Storey*, the Second Circuit similarly held that where the Uniform Domain-Name Dispute-Resolution Policy ("UDRP") provided no definition for "court of competent jurisdiction" as a term of art, it gave the term its plain meaning; namely, a court that has jurisdiction to hear the claim brought before it. *Storey* at 380. Unlike the cases cited by MySpace, as noted above, here the term "court of competent jurisdiction" is clearly defined in the statute.

Both *Ins. Corp. of Ireland, Ltd. v. Compagnie des Bauxites de Guinee*, 456 U.S. 694 (1982) and *Sinoying Logistics Pte Ltd. v. Yi Da Zin Trading Corp.*, 619 F.3d 207 (2d. Cir. 2010) deal with the concept of a defendant being able to waive personal jurisdiction in a civil action, something that is wholly inapplicable in this matter. As best as Plaintiff can tell, MySpace seeks to ignore the specific definition of "court of competent jurisdiction" as set forth in 18 U.S.C. § 2711(3)(B) and instead argue that it can waive jurisdiction defenses and disclose personal and private user information, data, records and the contents of electronic communications in response to facially invalid warrants. Unfortunately for MySpace, the SCA is the statutory prohibition against such illegal behavior. MySpace's choice to waive valid legal process and disclose Plaintiff's information and content to law enforcement violates the SCA. In other words, it simply is not up to them, nor is it their right to waive MySpace Users' privacy protections. Although MySpace may *choose* to "waiv[e] jurisdictional defenses it may have to complying

with warrants faxed to it by courts in Georgia or elsewhere." (Def. Mem. at 11), every single time it does so MySpace becomes liable for civil damages for violating the SCA.

c. A Georgia Magistrate Court Cannot Issue a Search Warrant for a Search of Property Outside its County

A Cherokee County, Georgia, Magistrate Judge does not have jurisdiction to issue a search warrant – or otherwise authorize a search – respecting property outside its county, let alone outside the State of Georgia. The authority of any judicial officer in Georgia to issue a search warrant is limited to places within that court's territorial jurisdiction. *Lejeune*, 277 Ga. at 751-52, 594 S.E.2d at 638. Moreover, the lack of jurisdiction to issue a warrant results in a nullity. *State v. Kelley*, 302 Ga. App. 850, 691 S.E.2d 890 (Ga. Ct. App. 2010)); *see also Beck v. State*, 283 Ga. 352, 353, 658 S.E.2d 577, 579 (Ga. 2008) (citing *Pruitt v. State*, 123 Ga. App. 659, 182 S.E.2d 142 (Ga. Ct. App. 1971)("lack of jurisdiction to [enter or issue] warrant is not mere technicality, but results in a nullity")). Because the warrant in the instant matter purported to authorize a search in Beverly Hills, California, which is far beyond the territorial jurisdiction of Cherokee County, Georgia, the warrant was invalid, null and void on its face. Therefore, any disclosure made by MySpace allegedly in response thereto was an improper voluntary disclosure in violation of the SCA.

3. 18 U.S.C. § 2707(e) Requires Objective Reasonableness, *i.e.*, A Facially Valid Warrant

As noted above, the 18 U.S.C. § 2707(e) "good faith" defense, requires Defendant to show it was both subjectively and objectively reasonable for it to disclose plaintiff's subscriber information. *Freedman, supra,* at 648. Plaintiff submits the MySpace cannot meet this burden because it was both objectively and subjectively unreasonable for it to rely on a facially invalid warrant issued by a county magistrate judge in Georgia who was operating outside his

jurisdiction and otherwise lacked "general criminal jurisdiction" under Georgia law. Indeed MySpace, having made a public record of fervent and strict adherence to the ECPA and federal and state laws on proper judicial process, cannot now argue, as a matter of law, that it acted subjectively and objectively in good faith.

In *Freedman*, the Court granted partial summary judgment *for the plaintiff*, finding that he met the subjective component by showing that defendant acted knowingly in disclosing the prohibited personal information. *Id.* at 646. The court, however, denied the parties' cross motions for summary judgment on the issue of whether the knowing disclosure was reasonable "because there [was] a genuine issue of fact as to the objective reasonableness of [defendant]'s belief." *Id*. at 650. Those issues were better left to the trier of fact. *Id.* Contrary to Defendant's argument (Def. Mem. at 13), *Freedman* did not turn on whether the underlying warrant was signed or unsigned by a judge but rather whether: (i) defendant "had a subjective good faith belief that [it] disclosed plaintiff's subscriber information pursuant to a signed, valid warrant and (ii) that this belief was objectively reasonable in the circumstances." *Id*. at 648. Here, there remain significant factual issues as to whether MySpace was acting in good faith. This cannot be decided on a motion to dismiss.

In an attempt to support its claim to an 18 U.S.C. § 2707(e) good faith defense, Defendant cites four cases, all of which are easily distinguishable from the case at bar. Importantly, none of the cases cited by Defendant involve a county or state court subpoena, county or state search warrant, or county or state court order that purports to authorize a search beyond its jurisdictional reach.

In *Bansal v. Server Beach*, 285 Fed. Appx. 890, 892 (3d Cir. 2008) (per curiam), there was no question as to the validity of the federal court order pursuant to which the electronic

communications were divulged by Microsoft Corporation.[10] In *Bansal v. Microsoft Hotmail*, 267 Fed. Appx. 184 (3d Cir. 2008) (per curiam), which despite Defendant's characterization, does not involve any question as to the validity of the federal court order pursuant to which the emails and information concerning Bansal's account were disclosed to the government by Microsoft Hotmail. Additionally, unlike the disclosures by MySpace in the instant matter pursuant to § 2703, the court in *Bansal* found that Microsoft Hotmail made the disclosures pursuant to 18 U.S.C. § 2701(c), which provided Microsoft Hotmail an exception "because it is the communications service provider for his email account." *Id*. at 185. Again, contrary to Defendant's implication, Bansal's claims against Microsoft Hotmail were dismissed as meritless pursuant to 28 U.S.C. § 1915(e) ***not*** 18 U.S.C. § 2707(e). *Id.*

Likewise, in *Jayne v. Sprint PCS*, 2009 WL 426117 (E.D. Cal. Mar. 26, 2009), the court addressed the 2703(e) defense, ***not*** the 2707(e) defense as alleged by Defendant, and found the provider was entitled to the defense under 2703(e) because of the statutory authorization for emergency circumstances disclosure contained in 18 U.S.C. § 2702(c)(4). Defendant does not and cannot contend the emergency circumstances exception applies in the instant matter.

In *McReady v. eBay, Inc.*, 453 F.3d 882 (7th Cir. 2006) the Seventh Circuit addressed the 2707(e) good faith defense in the context of a subpoena issued by a federal district court as opposed to a warrant issued by a county magistrate judge. Plaintiff concedes that there is no question that a federal district court is a "court of competent jurisdiction" to issue a subpoena under the SCA. The *McReady* court was careful to note that "[n]othing else gives any indication of irregularity sufficient to put eBay on notice that the subpoena was 'phony.'" *McReady* at 892.

[10] Contrary to Defendant's implication, Bansal's claims against Microsoft Corporation were dismissed as frivolous pursuant to 28 U.S.C. § 1915(e), dealing specifically with civil actions by

The same cannot be said of the warrant at issue here, which was not issued by a court of competent jurisdiction and was thus facially invalid. Because the flaws in the warrant were apparent on its face, Defendant cannot – and applying the standard applicable to an affirmative defense on a Motion to Dismiss, certainly cannot – prevail on the "good faith" defense under § 2707(e).

In this case, Defendant claims that the validity or facial invalidity of the warrant is irrelevant. That interpretation of the SCA is entirely inconsistent with the "good faith" defense contained in 18 U.S.C. § 2707(e). After all, what need would there be for a "good faith" defense if the validity of the warrant did not matter? *See Freedman*, 325 F. Supp. 2d at 646. Moreover, even if this Court were to ignore the SCA's actual specific inclusion in 18 U.S.C. § 2703 that the warrant be issued by a court of competent jurisdiction, the mere inclusion of a good faith defense by Congress, in and of itself, establishes that the SCA requires that the process be valid process.

D. Although the Practice of Law Enforcement Faxing Out-of-State Warrants to Providers is Widespread, It Still Violates the SCA

Plaintiff agrees with MySpace that the practice of Providers accepting and responding to search warrants faxed by law enforcement, including from out-of-state state courts, is widespread, and even further agrees with MySpace that 18 U.S.C. § 2703(g) specifically contemplates law enforcement officers not being present when the warrant is executed.[11] However, Plaintiff disagrees with MySpace's implication that if everyone is doing so, it must be

---

a *pro se* litigant filed *in forma pauperis*, not because he made claims similar to Plaintiff's herein or that the Court found such claims frivolous. *Id.*

[11] Interestingly, in footnote 7 of its brief, MySpace quotes an excerpt from page 134 of the U.S. Dep't of Justice, "Searching and Seizing Computers and Obtaining Electronic Evidence Manual," *available at* http://www.cybercrime.gov/ssmanual/03ssma.html, but fails to include language from page 133, which is specifically applicable to Plaintiff's claims and which states, in pertinent part, "State courts may also issue warrants under § 2703, but the statute does not give these warrants effect outside the limits of the courts' territorial jurisdiction."

acceptable. This lemming argument has no basis in law and should not be embraced by this Court. Plaintiff also disagrees with MySpace's claim that many courts have readily approved the practice of service providers accepting and responding to faxed subpoenas and warrants.

Although most federal search warrants obtained under Fed. R. Crim. P. 41 are limited to "a search of property . . . within the district" of the authorizing magistrate judge, search warrants under § 2703 may be issued by a federal "court with jurisdiction over the offense under investigation," even for records held in another district. *See United States v. Berkos*, 543 F.3d 392, 396-98 (7th Cir. 2008). In fact, very few courts have addressed, let alone approved that practice. Those courts that have approved the practice did so in a very limited context by addressing the interplay between Fed. R. Crim. P. 41 and 18 U.S.C. § 2703, and specifically addressed the issuance of federal warrants that were to be executed outside of the district of issuance. *See In re Search of Yahoo, Inc.*, 2007 WL 1539971, at *7 (D. Ariz. May 21, 2007) (Title 18 U.S.C. § 2703(a) authorizes a federal district court to issue out-of-district warrants for the seizure of electronically-stored communications); *In re Search Warrant*, 2005 WL 3844032, at *6 (M.D. Fla. Dec. 23, 2005) ("Congress intended 'jurisdiction' to mean something akin to territorial jurisdiction"); *see also*, *United States v. Kernell*, 2010 WL 1408437, at *1 (E.D. Tenn. Apr. 2, 2010) ("[T]he statutory language of 18 U.S.C. § 2703 specifically authorizes the issuance of [search warrants for electronic communications and evidence to be executed out of the district]."), Report and Recommendation adopted by, 2010 WL 1491861 (April 13, 2010); *In re Application by the United States of Am. for a Search Warrant*, 665 F. Supp. 2d 1210 (D. Or. 2009).

MySpace is correct that California, Minnesota and Virginia,[12] each have laws governing corporations incorporated in their state, which require Providers incorporated in those states to disclose and produce information and records in response to warrants issued in other states. Unfortunately for MySpace, it is neither a California, nor Minnesota, nor Virginia, nor Massachusetts corporation, but rather a Delaware corporation. Neither Delaware nor any of the other 45 states, nor the District of Columbia, nor Puerto Rico, have similar statutes requiring Providers incorporated in those states to disclose and produce information and records in response to warrants issued in other states, and, as such, the statutes in those four states are the exception, rather than the rule. Moreover, despite Defendant's nonsensical argument, the fact that those specific states have statutes expressly requiring Providers incorporated in their states to disclose and produce to law enforcement information and records in response to warrants issued in other states, is proof in and of itself that the SCA prohibits MySpace's disclosures in the instant matter. Otherwise, those specific states would have no need for those disclosure statutes.

Defendant argues that California law expressly permits California corporations to accept out of state warrants. (Def. Mem. at 8). Defendant goes further and suggests that it would be an "absurd result" for the California legislature to intend to immunize California corporations and not all businesses doing business in California from accepting faxed warrants from out of state courts. *Id.* However, what Defendant omits to mention is that it appears that is exactly what the California legislature intended as it expressly excludes foreign corporations from such protection. *See* Cal. Penal Code § 1524.2(c). The law specifically delineates what actions

[12] Incidentally, the applicable statute in Virginia, Va. Code Ann. § 19.2-70.3, was amended in 2009, after the impermissible disclosure by MySpace in the instant matter. Additionally,

immunize California corporations and foreign corporations, respectively, and does not immunize foreign corporations from accepting warrants issued by another state. *See* Cal. Penal Code § 1524.2(d).

MySpace readily admits that no prior case has addressed the factual situation presented in Plaintiff's Amended Complaint. And, despite Defendant's arguments to the contrary, there remains a clear factual and legal distinction between a Provider's acceptance of a faxed federal search warrant as opposed to a search warrant issued by an out-of-state county magistrate court that lacks competent jurisdiction to issue such warrants and acts beyond its jurisdictional powers. Plaintiff respectfully submits that such actions are clearly violative of the SCA.

IV. CONCLUSION

For the foregoing reasons, Defendant's Motion to Dismiss should be denied.

Dated: March 17, 2011

Respectfully submitted,

HARWOOD FEFFER LLP

s/ Jeffrey M . Norton

Robert I. Harwood
Jeffrey M. Norton
488 Madison Ave.
New York, NY 10022
Telephone: (212) 935-7400
Facsimile: (212) 753-3630
rharwood@hfesq.com
jnorton@hfesq.com

although not cited by the Defendant, Massachusetts has a similar statute (Mass. Gen. Laws Ann. ch. 276 § 1B(d).

LAW OFFICE OF JOSHUA A. MILLICAN, P.C.
Joshua A. Millican
The Grant Building, Suite 607
44 Broad Street, N.W.
Atlanta, Georgia 30303
Telephone: (404) 522-1152
Facsimile: (404) 522-1133
joshua.millican@lawofficepc.com

BILLIPS & BENJAMIN LLP
Matthew C. Billips
One Tower Creek
3101 Towercreek Parkway, Suite 190
Atlanta, Georgia 30339
Telephone: (770) 859-0751
Facsimile: (770) 859-0752
billips@bandblawyers.com

GREENFIELD MILLICAN P.C.
Lisa T. Millican
607 The Grant Building
44 Broad Street, N.W.
Atlanta, Georgia 30303
Telephone: (404) 522-1122
Facsimile: (404) 522-1133
lisa.millican@lawofficepc.com

Counsel for Plaintiff

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CORY HUBBARD, individually, and on behalf of a class of all others similarly situated, **Plaintiff,** **v.** **MYSPACE, INC.,** **Defendant.**	**Index No.: 11-cv-00433 (LAK)** **ECF CASE**

CERTIFICATE OF SERVICE

The undersigned hereby certifies that this 17th day of March, 2011, I electronically filed Plaintiff's Memorandum of Law in Response and Opposition to MySpace, Inc.'s Motion to Dismiss with the Clerk of Court in the United States District Court, for the Southern District of New York, using the CM/ECF system, which will automatically send email notification of such filing to all attorneys of record.

Dated: March 17, 2011

s/ Jeffrey M . Norton

Jeffrey M. Norton
HARWOOD FEFFER LLP
488 Madison Ave.
New York, NY 10022
Telephone: (212) 935-7400
Facsimile: (212) 753-3630
jnorton@hfesq.com