

**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.

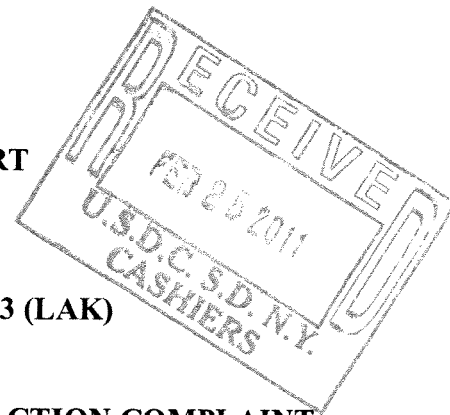
MYSFACE, INC.,

Defendant.

Index No.: 11-cv-00433 (LAK)

AMENDED CLASS ACTION COMPLAINT

ECF CASE



Plaintiff Cory Hubbard (“Plaintiff”), individually and on behalf of a class of all others similarly situated (the “Class”), brings this action against MySpace, Inc. (“MySpace” or “Defendant”). Plaintiff’s allegations are based upon knowledge as to his own acts and upon information and belief as to all other matters. Plaintiff’s information and belief is based upon, among other things, an investigation undertaken by his counsel, which included, without limitation: (a) interviews of witnesses, (b) review of the Company’s published materials and information available on the internet; and (c) analysis of public records and documents. Plaintiff believes that additional substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

PRELIMINARY STATEMENT

1. This is a class action lawsuit against MySpace for improperly and voluntarily disclosing certain personal and private user information, data, records and/or the contents of

electronic communications in violation of the privacy rights of visitors, members, subscribers, customers or users of MySpace services (“MySpace Users”).

2. As alleged herein, MySpace disclosed personal and private user information, data, records and/or 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.

3. The impermissibly disclosed personal and private user information, data, records and/or 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.

4. MySpace’s unlawful disclosure of personal and private user information, data, records and/or the contents of electronic communications violates MySpace Users’ rights under federal and state statutes as well as common law.

5. Plaintiff, on behalf of himself and all other similarly situated, seeks monetary damages, including statutory damages, punitive damages, equitable relief, attorneys’ fees and expenses of litigation.

PARTIES

6. 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 in violation of federal and state statutes and common law.

7. Defendant MySpace, Inc. is a Delaware corporation that has its principal place of business located at 407 N. Maple Drive in Beverly Hills, California 90210. MySpace does business and operates throughout the United States and may be properly served through its registered agent of service, CT Corporation System at 818 W. 7th Street in Los Angeles, California 90017.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and 1332(d) because the amount in controversy exceeds \$5,000,000.00 exclusive of interest and costs, and more than two-thirds of the users of the putative class are citizens of states different than that of MySpace. Additionally, the Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331.

9. Defendant MySpace is subject to the jurisdiction of this Court and venue is proper as a result of a choice of forum provision in MySpace's Terms of Use Agreement, which provides, in relevant part, "The Agreement shall be governed by, and construed in accordance with, the laws of the State of New York, without regard to its conflict of law provisions. You and MySpace agree to submit to the exclusive jurisdiction of the courts located within the State of New York to resolve any dispute arising out of the Agreement or the MySpace Services."

STATEMENT OF FACTS

10. 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.

11. The Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("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.

12. MySpace encourages MySpace Users to share personal and private user information and data. In its Terms of Use Agreement and MySpace Privacy Policy (collectively the "Agreement"), MySpace claims it protects MySpace Users' privacy as required by law and applicable privacy policies.

13. MySpace hired Hemanshu Nigam as its Chief Security Officer in 2006.

14. 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.

15. In an interview as set forth on Exhibit A attached hereto and incorporated herein, 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.”

16. 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 since MySpace had acknowledged that it could not turn over the information under the terms of the ECPA because it agreed the ECPA prohibited such information from being shared without a subpoena, as well as some state privacy laws.

17. In a CNET News article, attached hereto as Exhibit B and incorporated herein by reference, Michael Angus, then the Executive Vice President and General Counsel of Fox Interactive Media, a parent company of MySpace, when speaking about the plan for MySpace’s cooperation provided, “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.”

18. In an interview with Reuters, attached hereto as Exhibit C and incorporated herein by reference, Mr. Angus provided further detail about MySpace’s plan to cooperate with law enforcement. Mr. Angus continued, “[e]ach state has its own laws...It’s an intricate web of laws that we make sure we comply with ...”

19. In a February 4, 2009, letter to the Honorable Roy Cooper, Attorney General of North Carolina, attached hereto as Exhibit D and incorporated herein by reference, 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.”

20. Recognizing the importance of the privacy rights of MySpace Users, in an interview with CNET in February 2010, attached hereto as Exhibit E and incorporated herein by reference, Mr. Nigam on behalf of MySpace further provided, “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.”

21. 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.”

22. In an interview in March 2010, attached hereto as Exhibit F and incorporated herein by reference, Mr. Nigam further provided 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.”

23. Although MySpace claims publicly that it protects MySpace Users’ privacy and conforms with the strict requirements of the applicable federal statutes and other laws when accessing or disclosing personal and private user information, data, records and/or the contents of electronic communications, MySpace routinely and unlawfully accepts as valid legal process from law enforcement and other government entities facsimile transmissions of state search warrants signed by state magistrates and other state judges.

24. State search warrants signed by state magistrates and other state judges have no force and effect outside the limits of that state courts’ territorial jurisdiction, and when faxed or

sent out of that state, said search warrants are invalid, unenforceable and not deemed issued by a court of competent jurisdiction.

25. MySpace's intentional disclosure of a MySpace User's personal and private user information, data, records and/or the contents of electronic communications in response to a foreign state search warrant is improper and violative of federal and state law.

26. Although MySpace claims publicly that it protects MySpace Users' privacy and conforms with the strict requirements of the applicable federal statutes and other laws when releasing personal and private user information, data, records and/or the contents of electronic communications, MySpace routinely and unlawfully accepts as valid legal process from law enforcement and other government entities facsimile transmissions of state grand jury or trial subpoenas, sometimes with express instructions on the face of the state subpoena to not provide notice of the subpoena to the MySpace User.

27. State grand jury or trial subpoenas have no force and effect outside of the state of issuance, and when faxed or sent out of state, said subpoenas are invalid and unenforceable.

28. MySpace's intentional disclosure of a MySpace User's personal and private user information, data, records and/or the contents of electronic communications in response to a state grand jury or trial subpoena is improper and violative of federal and state law.

29. Although MySpace claims publically that it protects MySpace Users' privacy and conforms with the strict requirements of the applicable federal statutes and other laws when accessing or disclosing personal and private user information, data, records and/or the contents of electronic communications, MySpace routinely and unlawfully discloses personal and private user information, data, records and/or the contents of electronic communications in response to

letter requests from law enforcement and other government entities in lieu of proper valid legal process.

30. The letters from law enforcement and other government entities requesting personal and private user information, data, records and/or the contents of electronic communications referenced in the preceding paragraph are neither warrants 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, nor administrative subpoenas authorized by a Federal or State statute, nor Federal or State grand jury or trial subpoenas nor a court order issued by a court of competent jurisdiction. Such letters do not constitute valid or enforceable legal process, which would require or permit MySpace to access or disclose personal and private user information and data.

31. MySpace's intentional disclosure of a MySpace User's personal and private user information, data, records and/or the contents of electronic communications in response to letter requests is improper and violative of federal and state law.

32. MySpace's disclosure of Plaintiff Hubbard's personal and private user information, data, records and/or the contents of electronic communications data is representative of the unlawful disclosures of personal and private user information, data, records and/or the contents of electronic communications at issue in this lawsuit.

33. On January 16, 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.

34. The state search warrant was facially invalid and unenforceable, as it was not properly served on MySpace.

35. The state search warrant was facially invalid and unenforceable, as it purported to authorize a search by law enforcement of property outside the State of Georgia.

36. The state search warrant was facially invalid and unenforceable, as it purported to authorize a search by law enforcement of a witness outside the State of Georgia.

37. The state search warrant was facially invalid and unenforceable, as it purported to authorize a seizure by law enforcement of property outside the State of Georgia.

38. The state search warrant was facially invalid and unenforceable, as it purported to require and compel a response from the Custodian of Records of MySpace.com, a witness outside the State of Georgia.

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

CLASS ACTION ALLEGATIONS

40. Plaintiff brings this action on behalf of himself and the following Class:

All individuals in the United States, who are or were MySpace Users, and who have had personal and private user information, data, records and/or the contents of electronic communications in or regarding their MySpace accounts disclosed by MySpace to law enforcement and other government entities, without the MySpace Users' knowledge or authorization and without and not in response to a valid subpoena, warrant or Court order at any time from January 20, 2006, to the present (the "Class Period").

41. The Class is composed of numerous people, whose joinder in this action would be impracticable. The disposition of their claims through this class action will benefit Class members, the parties and the Courts. Upon information and belief, there are hundreds, if not thousands, of persons in the Class, and the actual number, identities and contact information of the individual members of the Class can be ascertained through MySpace's records.

42. There is a well-defined community of interest in questions of law and fact affecting the Class. These questions of law and fact predominate over individual questions affecting individual Class members, including, but not limited to, the following:

- a. whether MySpace disclosed to law enforcement and other government entities personal and private user information, data, records and/or the contents of electronic communications regarding Class members and their MySpace accounts;
- b. whether MySpace disclosed to law enforcement and other government entities personal and private user information, data, records and/or the contents of electronic communications regarding Class members and their MySpace accounts without a valid and enforceable search warrant;
- c. whether MySpace disclosed to law enforcement and other government entities personal and private user information, data, records and/or the contents of electronic communications regarding Class members and their MySpace accounts without and not in response to a valid and enforceable grand jury subpoena;

- d. whether MySpace disclosed to law enforcement and other government entities personal and private user information, data, records and/or the contents of electronic communications regarding Class members and their MySpace accounts without and not in response to a valid and enforceable Court order;
- e. whether MySpace's conduct described herein violates the SCA;
- f. whether Class members are entitled to damages as a result of MySpace's conduct described herein, and if so, what is the measure of those damages;
- g. whether Class members are entitled to statutory damages as a result of MySpace's conduct described herein, and if so, what is the measure of those statutory damages; and
- h. whether Class members are entitled to injunctive, declarative and monetary relief as a result of MySpace's conduct described herein.

43. Plaintiff's claims are typical of the claims of the members of the Class because Plaintiff and the other members of the Class each sustained damages arising out of MySpace's wrongful conduct as complained of herein. MySpace engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Class members. Similar or identical statutory and common law violations, business practices and injuries are involved. Individual questions, if any, pale by comparison to the numerous common questions that dominate.

44. The injuries sustained by the Class members flow from a common nucleus of operative facts. In each case, MySpace disclosed to law enforcement and other government entities personal and private user information, data, records and/or the contents of electronic

communications regarding Class members and their MySpace accounts without valid and enforceable legal process.

45. Given the similar nature of the Class members' claims and absence of material differences in the statutes and common law upon which the Class members' claims are based, a nationwide class will be easily managed by the Court and the parties as the identities of the Class members are known to MySpace, and damages, including the applicable statutory damages, can be calculated to a reasonable certainty.

46. Because of the relatively small size of the Class members' claims and given the significant expense required to prosecute the foregoing claims against MySpace, no Class member could afford to seek legal redress on an individual basis.

47. Plaintiff is not aware of any litigation concerning this controversy that has already been initiated by any members of this Class.

48. Plaintiff's claims are typical of those of the Class as all members of the Class are similarly affected by MySpace's uniform and actionable conduct described herein.

49. MySpace has acted and failed to act on grounds generally applicable to Plaintiff and other Class members requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class members.

50. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class action and complex litigation. Plaintiff has no interests antagonistic to, or in conflict with, those of the Class they seek to represent.

51. Plaintiff reserves the right to revise the above class definition based on facts learned in discovery.

COUNT ONE

(Violation of the Stored Communications Act)

52. Plaintiff, on behalf of himself and the class, realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

53. The SCA sets forth a system of statutory privacy rights for customers and users of electronic communications service providers and remote computing service providers, such as MySpace.

54. The ECPA broadly defines an “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...” 18 U.S.C. § 2510(12).

55. MySpace’s Users’ personal and private user information, data, records, contact lists, friends, relationships, content of email communications, content of private messages in the MySpace User’s Inbox and sent mail folders, photos, videos, files, website posts, registration, email and other IP address information are electronic communications within the meaning of 18 U.S.C. § 2510(12).

56. The ECPA also broadly defines the contents of a communication as follows: “[C]ontents’, when used with respect to any wire, oral, or electronic communication, include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

57. An “electronic communications system” is “any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” 18 U.S.C. § 2510(14).

58. Pursuant to the ECPA, “electronic storage” means any “temporary storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17).

59. MySpace holds its MySpace Users’ personal and private user information, data, records, contact lists, friends, relationships, content of email communications, content of private messages in the MySpace User’s Inbox and sent mail folders, photos, videos, files, website posts, registration, email and other IP address information in electronic storage within the meaning of 18 U.S.C. § 2510(17).

60. An electronic communication service (“ECS”) is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

61. MySpace operates an ECS as defined in 18 U.S.C. § 2510(15).

62. A remote computing service (“RCS”) is “the provision to the public of computer storage or processing services by means of an electronic communications system.” 18 U.S.C. § 2711(2).

63. MySpace operates a RCS as defined in 18 U.S.C. § 2711(2).

64. 18 U.S.C § 2702 regulates voluntary disclosure by internet service providers of customer communications and records, including specific prohibitions.

65. Pursuant to the SCA, “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage on that service.” 18 U.S.C § 2702(a)(1).

66. Pursuant to the SCA “a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service.” 18 U.S.C § 2702(a)(2).

67. Pursuant to the SCA, “a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2) to any governmental entity.” 18 U.S.C § 2702(a)(3).

68. 18 U.S.C. § 2703 articulates the steps that law enforcement officers and other government entities must take to compel providers to disclose the content of stored wire or electronic communications and other personal and private user information and data such as account records and basic subscriber and session information.

69. Pursuant to 18 U.S.C. § 2703(a) “[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, 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.”

70. Pursuant to 18 U.S.C. § 2703(b)(1)(A), “[a] governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication...without required notice to the subscriber or customer, if the governmental entity obtains 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.”

71. Pursuant to 18 U.S.C. § 2703(b)(1)(B), “[a] governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication... with prior notice from the governmental entity to the subscriber or customer if the governmental entity-- (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or (ii) obtains a court order for such disclosure under [18 U.S.C. § 2703(d)].”

72. Pursuant to 18 U.S.C. § 2703(c)(1), “A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity-- (A) obtains 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; [or] (B) obtains a court order for such disclosure under [18 U.S.C. § 2703(d)]...”

73. Pursuant to 18 U.S.C. § 2703(c)(2), “A provider of electronic communication service or remote computing service shall disclose to a governmental entity the-- (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under [18 U.S.C. § 2703(c)(1)].”

74. Pursuant to 18 U.S.C. § 2703(c)(3), “A governmental entity receiving records or information under [18 U.S.C. § 2703(c)] is not required to provide notice to a subscriber or customer.”

75. Pursuant to 18 U.S.C. § 2703(d), “[a] court order for disclosure under [18 U.S.C. § 2703(b)] or [18 U.S.C. § 2703(c)] may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation [and] [i]n the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.”

76. State search warrants, however, signed by state magistrates and other state judges are invalid, unenforceable and have no force and effect outside the limits of that state courts’

territorial jurisdiction, and therefore those state search warrants are not issued by a court of competent jurisdiction.

77. MySpace's disclosure of a MySpace User's personal and private user information, data and the contents of electronic communications in response to or in lieu of a response to a foreign state search warrant is improper and violative of the SCA.

78. By disclosing a MySpace User's personal and private user information, data and the contents of electronic communications in response to or in lieu of a response to a foreign state search warrant that has no force and effect outside the limits of that state courts' territorial jurisdiction, MySpace knowingly, willfully, unlawfully, intentionally and without authorization divulged the contents of communications while those communications were maintained in electronic storage in violation of 18 U.S.C. §2702(a)(1).

79. State grand jury or trial subpoenas are invalid, unenforceable and have no force and effect outside of the state of issuance and cannot be used or served in another state to compel a provider in the foreign state to give testimony or produce records.

80. MySpace's disclosure of a MySpace User's personal and private user information, data and the contents of electronic communication in response to or in lieu of response to a foreign state grand jury or trial subpoena is improper and violative of the SCA.

81. By disclosing a MySpace Users' personal and private user information, data and the contents of electronic communications in response to or in lieu of a response to a foreign state grand jury or trial subpoena that is invalid, unenforceable and has no force and effect outside of the state of issuance, MySpace knowingly, willfully, unlawfully, intentionally and

without authorization divulged the contents of communications while those communications were maintained in electronic storage in violation of 18 U.S.C. §2702(a)(1).

82. MySpace carries and maintains its MySpace Users' personal and private user information and data, contact lists, friends, relationships, content of email communications, content of private messages in the MySpace User's Inbox and sent mail folders, photos, videos, files, website posts, registration, email and other IP address information on behalf of the MySpace Users.

83. MySpace carries and maintains some of its MySpace Users' personal and private user information and data, contact lists, friends, relationships, content of email communications, content of private messages in the MySpace User's Inbox and sent mail folders, photos, videos, files, website posts, registration, email and other IP address information solely for the purpose of providing storage and computer processing services to its users. MySpace is not authorized to access this information for purposes other than providing storage and computer processing.

84. By engaging in the foregoing acts and omissions, MySpace knowingly, willfully, unlawfully, intentionally and without authorization divulged the contents of communications that are carried and maintained by MySpace on behalf of, and received by transmission from, MySpace Users in violation of 18 U.S.C. § 2702(a)(2).

85. MySpace's knowing, willful, unlawful, and intentional disclosure of the contents of communications that are carried and maintained by MySpace on behalf of, and received by transmission from, MySpace Users was not made pursuant to any exceptions to the prohibitions against disclosure as set forth in 18 U.S.C. § 2702(b).

86. MySpace also engaged in the foregoing acts and omissions without first being served with a valid and enforceable warrant issued by a court of competent jurisdiction as required by 18 U.S.C. § 2703(a) or 18 U.S.C. § 2703(b)(1)(A).

87. MySpace also engaged in the foregoing acts and omissions without first being served with a valid and enforceable Federal or State grand jury or trial subpoena and with prior notice from the government entity to the subscriber or customer as required by 18 U.S.C. § 2703(b)(1)(B)(i).

88. MySpace also engaged in the foregoing acts and omissions without first being served with a valid and enforceable Federal or State grand jury or trial subpoena as required by 18 U.S.C. § 2703(c)(2).

89. MySpace also engaged in the foregoing acts and omissions without first being served with a valid and enforceable administrative subpoena authorized by a Federal or State statute and with prior notice from the government entity to the subscriber or customer as required by 18 U.S.C. § 2703(b)(1)(B)(i).

90. MySpace also engaged in the foregoing acts and omissions without first being served with a valid and enforceable administrative subpoena authorized by a Federal or State statute as required by 18 U.S.C. § 2703(c)(2).

91. MySpace also engaged in the foregoing acts and omissions without first being served with a valid and enforceable court order issued by a court of competent jurisdiction and with prior notice from the government entity to the subscriber or customer as required by 18 U.S.C. § 2703(b)(1)(B)(ii) and 18 U.S.C. § 2703(d).

92. MySpace engaged in the foregoing acts and omissions without first being served with a valid and enforceable court order issued by a court of competent jurisdiction as required by 18 U.S.C. § 2703(c)(1)(B) and 18 U.S.C. § 2703(d).

93. None of the foregoing acts and omissions taken by MySpace were permissible pursuant to any exceptions to the prohibition against disclosure as set forth in 18 U.S.C. § 2701(c).

94. None of the foregoing acts and omissions taken by MySpace were permissible pursuant to any exceptions to the prohibition against disclosure as set forth in 18 U.S.C. § 2702(b).

95. None of the foregoing acts and omissions taken by MySpace were permissible pursuant to any exceptions to the prohibition against disclosure as set forth in 18 U.S.C. § 2702(c).

96. None of the foregoing acts and omissions taken by MySpace was in accordance with the requirement of a valid and enforceable court order under the SCA as to preclude a cause of action against MySpace as set forth in 18 U.S.C. § 2703(e).

97. None of the foregoing acts and omissions taken by MySpace was in accordance with the requirement of a valid and enforceable warrant under the SCA as to preclude a cause of action against MySpace as set forth in 18 U.S.C. § 2703(e).

98. None of the foregoing acts and omissions taken by MySpace was in accordance with the requirement of a valid and enforceable subpoena under the SCA as to preclude a cause of action against MySpace as set forth in 18 U.S.C. § 2703(e).

99. None of the foregoing acts and omissions taken by MySpace was in accordance with the requirement of a valid and enforceable statutory authorization under the SCA as to preclude a cause of action against MySpace as set forth in 18 U.S.C. § 2703(e).

100. None of the foregoing acts and omissions taken by MySpace was in accordance with the requirement of a valid and enforceable certification under the SCA as to preclude a cause of action against MySpace as set forth in 18 U.S.C. § 2703(e).

101. None of the foregoing acts and omissions taken by MySpace was in accordance with the requirement of a valid and enforceable legal process or anything else under the SCA as to preclude a cause of action against MySpace as set forth in 18 U.S.C. § 2703(e).

102. None of the foregoing acts and omissions taken by MySpace were based on a valid and enforceable grand jury subpoena or a good faith reliance on the same so as to constitute a complete defense to this civil action as set forth in 18 U.S.C. § 2707(e).

103. None of the foregoing acts and omissions taken by MySpace were based on a valid and enforceable court warrant or a good faith reliance on the same so as to constitute a complete defense to this civil action as set forth in 18 U.S.C. § 2707(e).

104. None of the foregoing acts and omissions taken by MySpace were based on a valid and enforceable court order or a good faith reliance on the same so as to constitute a complete defense to this civil action as set forth in 18 U.S.C. § 2707(e).

105. None of the foregoing acts and omissions taken by MySpace were based on a valid and enforceable legislative authorization or a good faith reliance on the same so as to constitute a complete defense to this civil action as set forth in 18 U.S.C. § 2707(e).

106. None of the foregoing acts and omissions taken by MySpace were based on a valid and enforceable statutory authorization or a good faith reliance on the same so as to constitute a complete defense to this civil action as set forth in 18 U.S.C. § 2707(e).

107. None of the foregoing acts and omissions taken by MySpace were based on valid and enforceable legal process or anything else or a good faith reliance on the same so as to constitute a complete defense to this civil action as set forth in 18 U.S.C. § 2707(e).

108. Each incident in which MySpace divulged personal and private user information, data, records and/or the contents of electronic communications of MySpace Users is a separate and distinct violation of the SCA.

109. MySpace's disclosures of its MySpace Users' personal and private user information, data, records and/or the contents of electronic communications were willful and intentional.

110. Plaintiff, on behalf of himself and the Class, is entitled to appropriate relief, including preliminary and other equitable or declaratory relief as this court may deem appropriate pursuant to 18 U.S.C. § 2707(b)(1).

111. Plaintiff, on behalf of himself and the Class, is entitled to a reasonable attorneys' fees and other litigation costs reasonably incurred as provided by 18 U.S.C. § 2707(b)(3).

112. Plaintiff, on behalf of himself and the Class, is entitled to recover monetary damages including actual damages, and statutory damages in the amount of not less than \$1,000.00 per Class member as provided by 18 U.S.C. § 2707(c).

113. Plaintiff, on behalf of himself and the Class, is entitled to recover punitive damages as provided by 18 U.S.C. § 2707(c).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays that the Court enter judgment and grant the following relief to Plaintiff and the Class:

(a) Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as class representative, and appoint his counsel as class counsel pursuant to Rule 23 of the Federal Rules of Civil Procedure;

(b) Declare that MySpace's actions, as described herein, violate the SCA (18 U.S.C. § 2701 *et seq.*);

(c) Award injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including, *inter alia*, an order prohibiting MySpace from engaging in the wrongful and unlawful acts described herein;

(d) Award damages, including statutory damages where applicable, to Plaintiff and the Class in an amount to be determined at trial;

(e) Award all economic, monetary, actual, consequential, and compensatory damages caused MySpace's conduct, and if its conduct is proved willful, award Plaintiff and the Class exemplary damages;

(f) Award restitution against MySpace for all money to which Plaintiff and the Class are entitled in equity;

(g) Award Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

(h) Award Plaintiff and the Class pre-judgment and post-judgment interest, to the extent allowable; and

(i) Award such other and further relief allowed by law as the Court deems just and proper.

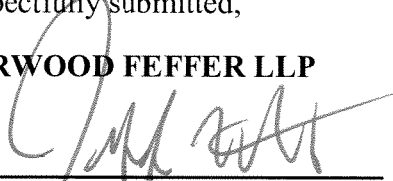
JURY DEMAND

Plaintiff demands a trial by jury.

Dated: February 25, 2011

Respectfully submitted,

HARWOOD FEFER LLP



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

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

EXHIBIT A



MySpace won't give names of sex offenders

Online networking site says proper legal processes weren't followed

By Elizabeth Dunbar

AP Associated Press

updated 5/16/2007 3:55:23 PM ET

RALEIGH, N.C. — Citing federal privacy law, MySpace.com said Tuesday it won't comply with a request by attorneys general from eight states to hand over the names of registered sex offenders who use the social networking Web site.

MySpace's chief security officer said the company regularly discloses information to law enforcement officials but the federal Electronic Communications Privacy Act says it can only do so when proper legal processes are followed.

"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," the security officer, Hemanshu Nigam, said in an interview.

In a letter Monday, attorneys general from North Carolina, Connecticut, Georgia, Idaho, Mississippi, New Hampshire, Ohio and Pennsylvania asked MySpace to provide information about registered sex offenders using the site and where they live.

Connecticut Attorney General Richard Blumenthal on Tuesday blasted MySpace for refusing to share the information and said no subpoena is needed for MySpace to tell the attorneys general how many registered sex offenders use the site "or other information relating to possible parole violations."

"I am deeply disappointed and troubled by this unreasonable and unfounded rejection of our request for critical information about convicted sex offenders whose profiles are on MySpace," Blumenthal said. "By refusing this information, MySpace is precluding effective enforcement of parole and probation restrictions that safeguard society."

Christian Genetski, an attorney who has represented MySpace, said the Electronic Communications Privacy Act requires subpoenas, court orders or search warrants, depending on the information sought.

"It's a clearly defined law that most providers and prosecutors understand and work with on a daily basis," Genetski said. "My understanding is (the attorneys general) want the private personal information, and that's clearly the information the ECPA protects."

North Carolina Attorney General Roy Cooper said "it's sad that MySpace is going to protect

advertisement

GROUPON

62% OFF

The Daily Deal - Atlanta \$25 for Oil Change, New Wiper Blades, and Tire Rotation at Catherine's Auto Repair (\$65 Value)

GET DEAL AT: 

www.PrintGroupon.com/383351

Time Sensitive Offer

Print Powered By 



the privacy of sex offenders over the safety of children.”

Nigam said MySpace is serious about identifying and removing sex offenders from its Web site and wants to work with the attorneys general.

“Everybody needs to get together and delete online predators,” Nigam said, adding that MySpace supports state and federal legislation requiring sex offenders to register e-mail addresses. “The attorneys general’s concerns and our concerns are exactly the same.”

In December, MySpace announced it was partnering with Sentinel Tech Holding Corp. to build a database with information on sex offenders in the United States.

Software to identify and remove sex offenders from the site has been used for 12 days, and MySpace has “removed every registered sex offender that we identified out of our more than 175 million profiles,” Nigam said.

It is also working with Sentinel to share the sex offender database and technology with the National Center for Missing and Exploited Children, which works directly with law enforcement officials, Nigam said.

MySpace, which is owned by News Corp., and other social networking sites allow users to create online profiles with photos, music and personal information, including hometowns and education. Users can send messages to one another and, in many cases, browse other profiles.

MySpace’s policy prevents children under 14 from setting up profiles, but it relies on users to specify their ages.

© 2011 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

advertisement

HEARTLAND QUALITY
OMAHA STEAKS
SINCE 1917

SAVE
up to **64%**
to

Plus, get
3 FREE Gifts

Special Code: **45069ZWN**

To order: www.OmahaSteaks.com/print71
or call 1-877-605-0496

Print Powered By FormatDynamics™

EXHIBIT B

CNET News

[CNET News](#)

- [log in](#)
- [join CNET](#)
- [Home](#)
- [Reviews](#)
- [You are here:News](#)
- [Downloads](#)
- [Video](#)

Search

- [Latest News](#)
- [CNET River](#)
- [Latest News](#)
- [Webware](#)
- [Crave](#)
- [Business Tech](#)
- [Green Tech](#)
- [Wireless](#)
- [Security](#)
- [Blogs](#)
- [Video](#)
- [Photos](#)
- [More Menu](#)

May 21, 2007 9:19 AM PDT

MySpace to provide sex offender data to state AGs

By [Caroline McCarthy](#)

Staff Writer, CNET News

Last modified: May 21, 2007 3:08 PM PDT

Welcome Google user!

More headlines related to ["MySpace to provide sex offender data to state AGs"](#):

Add CNET News to Google

- [Two decades in prison for Iranian blogger](#)
- [A user's guide to robotics higher ed](#)
- [Look out, Rover. Robots are man's new best friend](#)
- [Why are doctors such Luddites?](#)
- [More matching headlines »](#)

Add CNET News headlines to your Google homepage or Google reader.

[Google](#)



MySpace.com unveiled a plan Monday for cooperating with requests from state attorneys general for data

pertaining to registered sex offenders.

According to a statement from the company, MySpace will provide the Multi-State Attorney General Executive Committee with data from Sentinel Safe, the database of information on registered sex offenders that the company has compiled through its partnership with identity verification firm [Sentinel Tech Holding](#).

Sentinel Safe, which

Related Stories

[Protecting kids from online food ads](#)
May 17, 2007

[Feud between MySpace, state AGs heats up](#)
May 16, 2007

[State AGs to MySpace: Turn over sex offender data](#)
May 14, 2007

contains data aggregated from state registries, has been in the works since late last year and was officially deployed May 2.

The key behind the new plan, according to MySpace representatives, is efficiency. "There were more than 50 disparate sex offender registries and no way of tying them together and checking them against our user database," Hemanshu Nigam, MySpace's chief security officer, said in an interview. So far, the software has flagged and deleted about 7,000 registered sex offenders from MySpace's user base of around 180 million profiles, according to Michael Angus, general counsel for MySpace parent company Fox Interactive Media, a subsidiary of News Corp.

"Up until now, the predators have felt like they can have a free ride (on social-networking sites), and that day is over," Angus said.

MySpace initially asserted that it was legally unable to comply with the requests set forth in [a letter sent earlier this month](#) from the attorneys general of eight states--Connecticut, Georgia, Idaho, Mississippi, New Hampshire, North Carolina, Ohio and Pennsylvania. The letter asking that the social-networking site provide the data, cited concerns "that sexual predators are using MySpace to lure children into face-to-face encounters and other dangerous activities."

But MySpace responded that [it couldn't](#) turn the information over due to the terms of the [Electronic Communications Privacy Act](#) of 1986, which technically prohibits such information from being shared without a subpoena, as well as some state privacy laws.

It appears, however, that an accord was struck late last week. Through MySpace's newly announced partnership with the attorneys general, Angus and Nigam said, the company will be able to address the federal and state laws. Company representatives emphasized that the social network had always planned to share the Sentinel Safe data with the attorneys, who could then pass the information on to law enforcement officials in their states.

Different hoops in different states

"It's simply a matter of making sure we jump through the right legal hoops," Angus said. In some states, that means civil subpoenas; in others, it means demands for investigation or other forms of court orders. "The process is really just compliance with each of the state laws, so each state has their own process that they have to follow," he said.

He added that the dialogue has been ongoing. "We have a long working history with the attorneys general, especially Richard Blumenthal (of Connecticut) and Roy Cooper (of North Carolina). We've been working with them for quite a while and they're aware that we've been developing this technology."

Harsh words came from the attorneys' offices last week. Blumenthal put out a statement saying it was "inexplicable and inexcusable" for MySpace to claim it was illegal to turn over the data, and Cooper said it was "outrageous that MySpace chooses to protect the privacy of predators over the safety of children."

A statement from Cooper on Monday confirmed that MySpace will be sharing the Sentinel Safe information with his office and those of the other attorneys general. "We're pleased to see MySpace step up to the plate and provide us with this very important information," the attorney general is

quoted as saying. Cooper is also, according to the release, promoting a new law in North Carolina to require parental consent for children to join sites like MySpace and ban sex offenders from belonging to social-networking sites altogether.

Connecticut's attorney general, Richard Blumenthal, conveyed a similar message in a separate statement Monday. "I am pleased that MySpace has heeded our demand, now by subpoena, to provide information about convicted sex offenders and confirm steps to remove them from the site," he said. "I commend MySpace for taking this step and welcome this cooperation."

MySpace, meanwhile, has been promoting other legal strategies to combat sex offenders. The site has been vocal in recommending that states mandate that all e-mail addresses belonging to registered sex offenders be kept on record. This practice has been signed into law in Kentucky, Virginia and Arizona, MySpace representatives said, and is being introduced in 13 other states. On the federal level, Senators Chuck Schumer (D-N.Y.) and John McCain (R-Ariz.) are pursuing similar legislation on the federal level.

This kind of law, Angus said, will allow MySpace to permanently block e-mail addresses that have been connected to sex offenders. "We need to criminalize their online activity," he said.

In addition, MySpace representatives said other social-networking sites will be able to license the Sentinel Safe database technology from the ID verification firm and use it to check their own membership records. Several companies, whose names were not disclosed, are apparently already in talks to do so. "We sense an urgency here," Angus said, "and the industry needs to participate in that sense of urgency."

See more CNET content tagged:

[MySpace](#), [Richard Blumenthal](#), [News Corp.](#), [attorney](#), [Hemanshu Nigam](#)

- [Reviews](#)
- [Cell Phones](#)
- [Camcorders](#)
- [Digital Cameras](#)
- [Laptops](#)
- [GPS](#)
- [TVs](#)
- [Car Tech](#)
- [All Reviews](#)

- [News](#)
- [Business Tech](#)
- [Corrections](#)

- [Crave](#)
- [Cutting Edge](#)
- [Green Tech](#)
- [Security](#)
- [Wireless](#)
- [All News](#)

- **Downloads**
- [Windows](#)
- [Mac](#)
- [Mobile](#)
- [Webware](#)
- [All Downloads](#)
- [Software deals](#)
- [Add your software](#)

- **Video**
- [Buzz Report](#)
- [CNET Top 5](#)
- [Loaded](#)
- [Prizefight](#)
- [Apple Byte](#)
- [All Videos](#)

- **More**
- [About CBS Interactive](#)
- [CNET Forums](#)
- [About CNET](#)
- [CNET Mobile](#)
- [CNET site map](#)
- [CNET Widgets](#)
- [Customer Help Center](#)
- [Newsletters](#)
- [Permissions](#)
- [RSS](#)

- **Join us on**
- [Facebook](#)
- [Twitter](#)
- [YouTube](#)

POPULAR TOPICS:

- [Apple iPhone](#)
- [Apple iPod](#)
- [LCD TV](#)

- [Apple iPad](#),
- [Smartphones](#),
- [Windows 7](#),
- [CES 2011](#),
- [Google Android](#),
- [HTC phones](#),
- [Android phones](#)


- [© 2011 CBS Interactive. All rights reserved.](#)
- [Privacy Policy](#)
- [Ad Choice](#)
- [Terms of Use](#)
- [Mobile User Agreement](#)
- Visit other CBS Interactive sites: 

EXHIBIT C



» Print

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to colleagues, clients or customers, use the Reprints tool at the top of any article or visit: www.reutersreprints.com.

MySpace in deal with 8 state attorneys general

Mon, May 21 2007

By Kenneth Li

NEW YORK (Reuters) - Popular Internet social network MySpace said on Monday it reached an accord with eight U.S. state attorneys general and has worked out a legal mechanism to hand over information on convicted sex offenders found on its service.

Last week, a coalition of U.S. law enforcement authorities criticized the News Corp.-owned service for not divulging information from profiles of convicted sex offenders on MySpace.

MySpace said it had identified, blocked and deleted about 7,000 such profiles, but had initially declined to hand over the information immediately, citing a disclosure law barring it from giving away the information without a court order.

By last Wednesday, MySpace and the attorneys general group reached an agreement.

MySpace officials said they had always intended to provide information to law enforcement officials, but were trying to work out a legal process for handing over the information.

"When we remove individuals from our site, we always keep in mind the law enforcement aspect of it," MySpace Chief Security Officer Hemanshu Nigam said in an interview.

MySpace and the attorneys general group, led by Connecticut Attorney General Richard Blumenthal and North Carolina AG Roy Cooper, have worked out a system to hand over information to be used to pursue offenders, although that process could differ from state to state.

"Each state has its own laws," Fox Interactive Media general counsel Mike Angus told Reuters. "It's an intricate web of laws that we make sure we comply with ... We don't want these guys walking out on a technicality."

Blumenthal said he has been issued a subpoena for the information. "Our subpoena compels this information right away -- within hours not weeks, without delay -- because it is vital to protecting children," he said in a statement. "Social networking sites should not be playgrounds for predators."

But some attorneys general urged the company to take more actions to protect minors.

"While conveying this information to us is a good first step, MySpace needs to do more, including implementing an effective age verification system that will make the site considerably safer," Ohio AG Marc Dann said in a statement.

MySpace has come under legal scrutiny over the past year after some of its young members fell prey to adult predators posing as minors. The families of several teenage girls who said they were sexually assaulted by MySpace members sued the service in January for failing to protect its members.

To protect its large audience of teenagers -- some as young as 14 years old -- MySpace late last year contracted background verification firm Sentinel Tech Holdings Corp. to develop the first national database of convicted sex offenders. MySpace uses the data to cross-reference against its own database of users and weed out predators.

Previously, registries of offenders were only available on a state level, making it difficult to track and investigate known offenders. The new system, called Sentinel SAFE, launched on May 2.

"We have zero tolerance for sex offenders," Angus said. "After spending a year meeting with AGs, we figured that if we were to move quickly, we had to build it ourselves."

Part of the dispute with legal authorities was over the term "deletion" of profiles, MySpace officials said. Although the service has deleted the profiles from MySpace, information is collected in its database for law enforcement, Angus said.

The attorneys general of Georgia, Idaho, North Carolina, Ohio, Pennsylvania, Mississippi and New Hampshire joined Connecticut in signing the letter last week demanding that the company turn over information on sex offenders on MySpace.



© Thomson Reuters 2011. All rights reserved. Users may download and print extracts of content from this website for their own personal and non-commercial use only. Republication or redistribution of Thomson Reuters content, including by framing or similar means, is expressly prohibited without the prior written consent of Thomson Reuters. Thomson Reuters and its logo are registered trademarks or trademarks of the Thomson Reuters group of companies around the world.

Thomson Reuters journalists are subject to an Editorial Handbook which requires fair presentation and disclosure of relevant interests.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to colleagues, clients or customers, use the Reprints tool at the top of any article or visit: www.reutersreprints.com.

EXHIBIT D



FOX INTERACTIVE MEDIA

407 South Staple Drive
Beverly Hills, California 90209
Phone 310 959 2029 • Fax 310 959 2027
e-mail: michael.angus@fox.com

Michael Angus
Executive Vice President
And General Counsel
Business and Legal Affairs

February 4, 2009

The Honorable Roy Cooper
Department of Justice
PO Box 629
Raleigh, NC 27602-0629

Dear General Cooper:

On February 3rd, we gladly provided the data we have been safeguarding in response to the subpoenas we received from Attorneys General Richard Blumenthal and Greg Abbott. They requested data on the 90,000 profiles of registered sex offenders (RSOs) that MySpace removed from our site since we implemented Sentinel SAFE two years ago. We are pleased to assist with these law enforcement efforts and look forward to the results of their investigations of the people who created these profiles.

No one else in the industry acts as aggressively as MySpace in this area, and we are proud of our industry leadership in creating a safer Internet. However, some of the comments surrounding news of our efforts have misconstrued our work and its results, and we want to clarify exactly why we created this program and what the numbers mean.

1. **90,000 RSO Profiles Removed:** Some reports wrongly suggested that there are 90,000 RSOs on MySpace today. This is wildly inaccurate and irresponsible. All 90,000 profiles were *removed* from MySpace upon discovery and preserved for law enforcement investigations. Such inaccurate reports send the message to other sites that they will be publicly criticized and punished for taking similar steps to protect teens online.

While much is being made of the increase in the number of RSOs removed from MySpace since the inception of our program, the fact is that as long as the program is working, the aggregate number of RSOs removed will increase – it is a cumulative number representing all of the profiles deleted over time. The program has been a tremendous success: not only have 90,000 RSOs been removed from MySpace, but MySpace has seen a 36 % reduction in RSOs attempting to access the site year over year.

2. **Subpoenas:** 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.
3. **Sentinel SAFE:** This is the tool MySpace uses to find and remove RSOs. After consulting with the Attorneys General in 2006, we worked with Sentinel

A NEWS CORPORATION COMPANY

The Honorable Roy Cooper
February 4, 2009
Page 2

Tech Holdings, Inc. to create this state-of-the-art RSO database that aggregates all publicly available RSO databases into one searchable solution. Nothing of its kind existed prior to that time. We compare each MySpace profile to the Sentinel SAFE RSO database on a 24/7 basis, and when we find a match, we delete the profile and preserve the information for you. Moreover, we donated the database to the National Center for Missing and Exploited Children so that the law enforcement community can use it as well.

4. **Industry Leader:** We are the only large scale site that finds and removes RSO profiles this aggressively. Others will never be able to remove the RSOs using their sites every day unless they adopt similar methods and tools. Today we are very concerned that the negative attention we receive for leading on safety actually discourages sites like Facebook from adopting similar technology to remove RSOs and make Facebook safer for its users. Instead of criticizing MySpace for leading the industry, we hope that you will call on Facebook to follow our lead and remove the thousands of RSOs that are now known to be on their site.

Working with the Attorneys General, MySpace has come a long way in safety, and we are proud to lead the industry in RSO removal and other areas. By accurately describing the productive safety efforts of MySpace and others, we can create a safer Internet together.

Sincerely,


Michael Angus

EXHIBIT E

CNET News
[CNET News](#)

- [log in](#)
- [join CNET](#)

- [Home](#)
- [Reviews](#)
- [You are here: News](#)
- [Downloads](#)
- [Video](#)

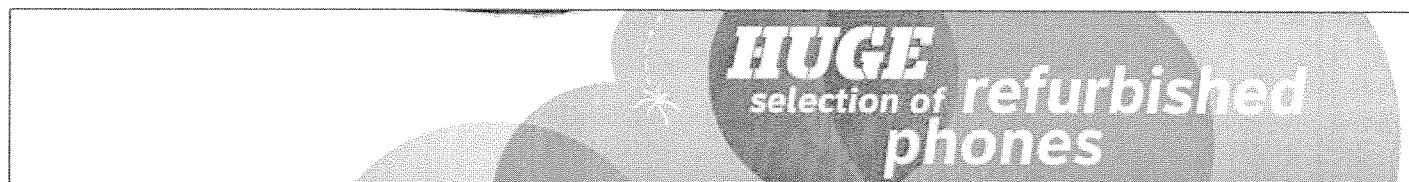
Search

Go

- [Latest News](#)
- [CNET River](#)
- [Latest News](#)
- [Webware](#)
- [Crave](#)
- [Business Tech](#)
- [Green Tech](#)
- [Wireless](#)
- [Security](#)
- [Blogs](#)
- [Video](#)
- [Photos](#)
- [More Menu](#)

[Politics and Law](#)

Ad Info ▼



February 3, 2010 4:00 AM PST

Police want backdoor to Web users' private data

by [Declan McCullagh](#)

2

[Share](#)

45



3 points

Anyone with an e-mail account likely knows that police can peek inside it if they have a paper search warrant.

But cybercrime investigators are frustrated by the speed of traditional methods of faxing, mailing, or e-mailing companies these documents. They're pushing for the creation of a national Web interface linking police computers with those of Internet and e-mail providers so requests can be sent and received electronically.

CNET has reviewed a survey scheduled to be released at a federal task force meeting on Thursday, which says that law enforcement agencies are virtually unanimous in calling for such an interface to be created. Eighty-nine percent of police surveyed, it says, want to be able to "exchange legal process requests and responses to legal process" through an encrypted, police-only "nationwide computer network." (See [one excerpt](#) and [another](#).)

The survey, according to two people with knowledge of the situation, is part of a broader push from law enforcement agencies to alter the ground rules of online investigations. Other components include renewed calls for laws [requiring Internet companies to store data](#) about their users for up to five years and increased pressure on companies to respond to police inquiries in hours instead of days.



But the most controversial element is probably the private Web interface, which raises novel security and privacy concerns, especially in the wake of a recent inspector general's [report \(PDF\)](#) from the Justice Department. The 289-page report [detailed](#) how the FBI obtained Americans' telephone records by citing nonexistent emergencies and simply asking for the data or writing phone numbers on a sticky note rather than following procedures required by law.

Some companies already have police-only Web interfaces. Sprint Nextel operates what it calls the L-Site, also known as the "legal compliance secure Web portal." The company even has offered a course that "will teach you how to create and track legal demands through L-site. Learn to navigate and securely download requested records." Cox Communications makes its [price list](#) for complying with police requests public; a 30-day wiretap is \$3,500.

The police survey is not exactly unbiased: its author is Frank Kardasz, who is scheduled to present it at a [meeting \(PDF\)](#) of the Online Safety and Technology Working Group, organized by the U.S.

Department of Commerce. Kardasz, a sergeant in the Phoenix police department and a project director of Arizona's Internet Crimes Against Children task force, said in an e-mail exchange on Tuesday that he is still revising the document and was unable to discuss it.

In an incendiary October 2009 essay, however, Kardasz wrote that Internet service providers that do not keep records long enough "are the unwitting facilitators of Internet crimes against children" and called for new laws to "mandate data preservation and reporting." He predicts that those companies will begin to face civil lawsuits because of their "lethargic investigative process."

"It sounds very dangerous," says Lee Tien, an attorney with the Electronic Frontier Foundation, referring to the police-only Web interface. "Let's assume you set this sort of thing up. What does that mean in terms of what the law enforcement officer be able to do? Would they be able to fish through transactional information for anyone? I don't understand how you create a system like this without it."

What police see in ISPs

Kardasz's survey, based on questionnaires completed by 100 police investigators, says that 61 percent of them had their investigations harmed "because data was not retained" and only 40 percent were satisfied with the timeliness of responses from Internet providers.

It also says: "89 percent of investigators agreed that a nationwide computer network should be established for the purpose of linking ISPs with law enforcement agencies so that they may exchange legal process requests and responses to legal process. Authorized users would communicate through encrypted virtual private networks in order to maintain the security of the data."

Some of the responses to other questions: "AT&T is very prompt." "Cox Communications seems to be the worst." "Places like Yahoo can take a month for basic subscriber info which is also a problem." "AT&T Mobility does not keep a log at all." "MySpace give (sic) me the quickest response and they have been very pro-police."

"You can be very supportive of law enforcement investigations and at the same time be very cognizant and supportive of the privacy rights of our users."

--Hemanshu Nigam, chief security officer, MySpace

Hemanshu (Hemu) Nigam, MySpace's chief security officer, said in an interview with CNET on Tuesday that: "You can be very supportive of law enforcement investigations and at the same time be very cognizant and supportive of the privacy rights of our users. 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."

Nigam said that MySpace accepts law enforcement requests through e-mail, fax, and postal mail, and that it has a 24-hour operations center that tries to respond to requests soon after they've been reviewed to make sure state and federal laws are being followed. MySpace does not have a police-only Web interface, he said.

Creating a national police-only network would be problematic, Nigam said. "I wish I knew the number of local police agencies in the country, or even police officers in the country," he said. "Right there that would tell you how difficult it would be to implement, even though ideally it would be a good thing."

Another obstacle to creating a nation-wide Web interface for cops--one wag has dubbed it "DragNet," and another "Porknet"--is that some of its thousands of users could be infected by viruses and other malware. Once an infected computer is hooked up to the national network, it could leak confidential information about ongoing investigations.

Jim Harper, a policy analyst at the free-market Cato Institute, says that he welcomes the idea of a police-only Web interface as long as it's designed carefully. "A system like this should have strong logins, should require that the request be documented fully, and should produce statistical information so there can be strong oversight," he says. "I think that's a good thing to have."



Declan McCullagh

Like 256

[Full Profile](#)

[E-mail Declan McCullagh](#)

Declan McCullagh is the chief political correspondent for CNET. Declan previously was a reporter for Time and the Washington bureau chief for Wired and wrote the Taking Liberties section and Other People's Money column for CBS News' Web site.

- [Reviews](#)
- [Cell Phones](#)
- [Camcorders](#)
- [Digital Cameras](#)
- [Laptops](#)
- [GPS](#)
- [TVs](#)

- [Car Tech](#)
- [All Reviews](#)

- **News**
- [Business Tech](#)
- [Corrections](#)
- [Crave](#)
- [Cutting Edge](#)
- [Green Tech](#)
- [Security](#)
- [Wireless](#)
- [All News](#)

- **Downloads**
- [Windows](#)
- [Mac](#)
- [Mobile](#)
- [Webware](#)
- [All Downloads](#)
- [Software deals](#)
- [Add your software](#)

- **Video**
- [Buzz Report](#)
- [CNET Top 5](#)
- [Loaded](#)
- [Prizefight](#)
- [Apple Byte](#)
- [All Videos](#)

- **More**
- [About CBS Interactive](#)
- [CNET Forums](#)
- [About CNET](#)
- [CNET Mobile](#)
- [CNET site map](#)
- [CNET Widgets](#)
- [Customer Help Center](#)
- [Newsletters](#)
- [Permissions](#)
- [RSS](#)

- **Join us on**
- [Facebook](#)
- [Twitter](#)
- [YouTube](#)

POPULAR TOPICS:


- [Apple iPhone](#),
 - [Apple iPod](#),
 - [LCD TV](#),
 - [Apple iPad](#),
 - [Smartphones](#),
 - [Windows 7](#),
 - [CES 2011](#),
 - [Google Android](#),
 - [HTC phones](#),
 - [Android phones](#)
-
- [© 2011 CBS Interactive. All rights reserved.](#)
 - [Privacy Policy](#)
 - [Ad Choice](#)
 - [Terms of Use](#)
 - [Mobile User Agreement](#)
 - Visit other CBS Interactive sites: 

EXHIBIT F



Break the Law and Your New 'Friend' May Be the FBI

Facebook feds go undercover: Report shows FBI, other agents dipping quietly into social media

By RICHARD LARDNER Associated Press Writer

WASHINGTON March 16, 2010 (AP)

The Feds are on Facebook. And MySpace, LinkedIn and Twitter, too.

U.S. law enforcement agents are following the rest of the Internet world into popular social-networking services, going undercover with false online profiles to communicate with suspects and gather private information, according to an internal Justice Department document that offers a tantalizing glimpse of issues related to privacy and crime-fighting.

Think you know who's behind that "friend" request? Think again. Your new "friend" just might be the FBI.

The document, obtained in a Freedom of Information Act lawsuit, makes clear that U.S. agents are already logging on surreptitiously to exchange messages with suspects, identify a target's friends or relatives and browse private information such as postings, personal photographs and video clips.

Among other purposes: Investigators can check suspects' alibis by comparing stories told to police with tweets sent at the same time about their whereabouts. Online photos from a suspicious spending spree — people posing with jewelry, guns or fancy cars — can link suspects or their friends to robberies or burglaries.

The Electronic Frontier Foundation, a San Francisco-based civil liberties group, obtained the Justice Department document when it sued the agency and five others in federal court. The 33-page document underscores the importance of social networking sites to U.S. authorities. The foundation said it would publish the document on its Web site on Tuesday.

With agents going undercover, state and local police coordinate their online activities with the Secret Service, FBI and other federal agencies in a strategy known as "deconfliction" to keep out of each other's way.

"You could really mess up someone's investigation because you're investigating the same person and maybe doing things that are counterproductive to

what another agency is doing," said Detective Frank Dannahey of the Rocky Hill, Conn., Police Department, a veteran of dozens of undercover cases.

A decade ago, agents kept watch over AOL and MSN chat rooms to nab sexual predators. But those text-only chat services are old-school compared with today's social media, which contain mountains of personal data, photographs, videos and audio clips — a potential treasure trove of evidence for cases of violent crime, financial fraud and much more.

The Justice Department document, part of a presentation given in August by top cybercrime officials, describes the value of Facebook, Twitter, MySpace, LinkedIn and other services to government investigators. It does not describe in detail the boundaries for using them.

"It doesn't really discuss any mechanisms for accountability or ensuring that government agents use those tools responsibly," said Marcia Hoffman, a senior attorney with the civil liberties foundation.

The group sued in Washington to force the government to disclose its policies for using social networking sites in investigations, data collection and surveillance.



ADVERTISEMENT

PRINT POWERED BY



Covert investigations on social-networking services are legal and governed by internal rules, according to Justice Department officials. But they would not say what those rules are.

The Justice Department document raises a legal question about a social-media bullying case in which U.S. prosecutors charged a Missouri woman with computer fraud for creating a fake MySpace account — effectively the same activity that undercover agents are doing, although for different purposes.

The woman, Lori Drew, helped create an account for a fictitious teen boy on MySpace and sent flirtatious messages to a 13-year-old neighborhood girl in his name. The girl hanged herself in October 2006, in a St. Louis suburb, after she received a message saying the world would be better without her.

A jury in California, where MySpace has its servers, convicted Drew of three misdemeanor counts of accessing computers without authorization because she was accused of violating MySpace's rules against creating fake accounts. But last year a judge overturned the verdicts, citing the vagueness of the law.

"If agents violate terms of service, is that 'otherwise illegal activity?'" the document asks. It doesn't provide an answer.

Facebook's rules, for example, specify that users "will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission." Twitter's rules prohibit its users from sending deceptive or false information. MySpace requires that information for accounts be "truthful and accurate."

A former U.S. cybersecurity prosecutor, Marc Zwillinger, said investigators should be able to go undercover in the online world the same way they do in the real world, even if such conduct is barred by a company's rules. But there have to be limits, he said.

In the face-to-face world, agents can't impersonate a suspect's spouse, child, parent or best friend. But online, behind the guise of a social-networking account, they can.

"This new situation presents a need for careful oversight so that law enforcement does not use social networking to intrude on some of our most personal relationships," said Zwillinger, whose firm does legal work for Yahoo and MySpace.

Undercover operations aren't necessary if the suspect is reckless. Federal authorities nabbed a man wanted on bank fraud charges after he started posting

Facebook updates about the fun he was having in Mexico.

Maxi Sopo, a native of Cameroon living in the Seattle area, apparently slipped across the border into Mexico in a rented car last year after learning that federal agents were investigating the alleged scheme. The agents initially could find no trace of him on social media sites, and they were unable to pin down his exact location in Mexico. But they kept checking and eventually found Sopo on Facebook.

While Sopo's online profile was private, his list of friends was not. Assistant U.S. Attorney Michael Scoville began going through the list and was able to learn where Sopo was living. Mexican authorities arrested Sopo in September. He is awaiting extradition to the U.S.

The Justice document describes how Facebook, MySpace and Twitter have interacted with federal investigators: Facebook is "often cooperative with emergency requests," the government said. MySpace preserves information about its users indefinitely and even stores data from deleted accounts for one year. But Twitter's lawyers tell prosecutors they need a warrant or subpoena before the company turns over customer information, the document says.

"Will not preserve data without legal process," the document says under the heading, "Getting Info From Twitter ... the bad news."

Twitter did not respond to a request for comment for this story.

The chief security officer for MySpace, Hemanshu Nigam, said MySpace doesn't want to be the company that stands in the way of an investigation.



ADVERTISEMENT

PRINT POWERED BY



"That said, we also want to make sure that our users' privacy is protected and any data that's disclosed is done under proper legal process," Nigam said.

MySpace requires a search warrant for private messages less than six months old, according to the company.

Facebook spokesman Andrew Noyes said the company has put together a handbook to help law enforcement officials understand "the proper ways to request information from Facebook to aid investigations."

The Justice document includes sections about its own lawyers. For government attorneys taking cases to trial, social networks are a "valuable source of info on defense witnesses," they said. "Knowledge is power. ... Research all witnesses on social networking sites."

But the government warned prosecutors to advise their own witnesses not to discuss cases on social media sites and to "think carefully about what they post."

It also cautioned federal law enforcement officials to think prudently before adding judges or defense counsel as "friends" on these services.

"Social networking and the courtroom can be a dangerous combination," the government said.

On the Net:

Justice Department cybercrime section: <http://www.justice.gov/criminal/cybercrime/>

Electronic Frontier Foundation: <http://www.eff.org>



ADVERTISEMENT

PRINT POWERED BY

