United States Senate

WASHINGTON, DC 20510

April 27, 2010

Mark Zuckerberg
Co-founder, CEO and President, Facebook
1601 S. California Avenue
Palo Alto, CA 94304

Dear Mr. Zuckerberg,

We are writing to express our concern regarding recent changes to the Facebook privacy policy and the use of personal data on third-party websites. While Facebook provides a valuable service to users by keeping them connected with friends and family and reconnecting them with long-lost friends and colleagues, the expansion of Facebook – both in the number of users and applications – raises new concerns for users who want to maintain control over their information.

The following three changes have raised concerns:

1. **Publicly available data**. Facebook's expansion of publicly available data to include a user's current city, hometown, education, work, likes, interests, and friends has raised concerns for users who would like to have an opt-in option to share this profile information. Through the expanded use of "connections," Facebook now obligates users to make publicly available certain parts of their profile that were previously private. If the user does not want to connect to a page with other users from their current town or university, the user will have that information deleted altogether from their profile. We appreciate that Facebook allows users to type this information into the "Bio" section of their profiles, and privatize it, but we believe that users should have more control over these very personal and very common data points. These personal details should remain private *unless* a user decides that he or she would like to make a connection and share this information with a community.

2. **Third-party data storage**. Previously, Facebook allowed third-party advertisers to store profile data for 24 hours. We are concerned that recent changes allow that data to be stored indefinitely. We believe that Facebook should reverse this policy, or at a minimum require users to opt in to allowing third parties to store data for more than 24 hours.

3. **Instant personalization.** We appreciate that Facebook is attempting to integrate the functionality of several popular websites, and that Facebook has carefully selected its initial partners for its new "instant personalization" feature. We are concerned, however, that this feature will now allow certain third-party partners to have access not only to a user's publicly available profile information, but also to the user's friend list and the

publicly available information about those friends. As a result of the other changes noted above, this class of information now includes significant and personal data points that should be kept private unless the user chooses to share them. Although we are pleased that Facebook allows users to opt-out of sharing private data, many users are unaware of this option and, moreover, find it complicated and confusing to navigate. Facebook should offer users the ability to opt in to sharing such information, instead of opting out, and should make the process for doing so more clear and coherent.

We hope that Facebook will stand by its goal of creating open and transparent communities by working to ensure that its policies protect the sensitive personal biographical data of its users and provide them with full control over their personal information. We look forward to the FTC examining this issue, but in the meantime we believe Facebook can take swift and productive steps to alleviate the concerns of its users. Providing opt-in mechanisms for information sharing instead of expecting users to go through long and complicated opt-out processes is a critical step towards maintaining clarity and transparency.

Sincerely,

Senator Charles E. Schumer

Senator Michael F. Bennet

Senator Mark Begich

Senator Al Franken

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

BLAKE J. ROBBINS, a Minor, by his Parents and Natural Guardians, **MICHAEL E. ROBBINS** and **HOLLY S. ROBBINS**, Individually, and on Behalf of all Similarly Situated Persons, 437 Hidden River Road Penn Valley, PA 19072-1112, Plaintiffs,	:	CIVIL ACTION
v.	:	NO.
LOWER MERION SCHOOL DISTRICT, 301 East Montgomery Avenue Ardmore, PA 19003, and **THE BOARD OF DIRECTORS OF THE LOWER MERION SCHOOL DISTRICT**, 301 East Montgomery Avenue Ardmore, PA 19003, and **CHRISTOPHER W. McGINLEY**, Superintendent of Lower Merion School District, 301 East Montgomery Avenue Ardmore, PA 19003, Defendants.	:	JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs, individually and on behalf of all similarly situated persons, by and through their undersigned attorneys, Lamm Rubenstone LLC, allege the following upon information and belief (except for those allegations pertaining to Plaintiffs, which are based on personal knowledge), after due investigation by undersigned counsel.

NATURE OF THE ACTION

1. Plaintiffs, Michael E. and Holly S. Robbins, bring this action on their own behalf and on behalf of their minor son, Blake J. Robbins, and as a Class Action on behalf of a class

consisting of Plaintiffs and all other students, together with their parents and families (the "Class"), who have been issued a personal laptop computer equipped with a web camera ("webcam") by the Lower Merion School District. Plaintiffs and the Class seek to recover damages caused to the Plaintiffs and Class by Defendants' invasion of Plaintiffs' privacy, theft of Plaintiffs' private information and unlawful interception and access to acquired and exported data and other stored electronic communications in violation of the Electronic Communications Privacy Act, The Computer Fraud Abuse Act, the Stored Communications Act, § 1983 of the Civil Rights Act, The Fourth Amendment of the United States Constitution, the Pennsylvania Wiretapping and Electronic Surveillance Act and Pennsylvania common law.

2. Unbeknownst to Plaintiffs and the members of the Class, and without their authorization, Defendants have been spying on the activities of Plaintiffs and Class members by Defendants' indiscriminant use of and ability to remotely activate the webcams incorporated into each laptop issued to students by the School District. This continuing surveillance of Plaintiffs' and the Class members' home use of the laptop issued by the School District, including the indiscriminant remote activation of the webcams incorporated into each laptop, was accomplished without the knowledge or consent of the Plaintiffs or the members of the Class.

3. Plaintiffs and the Class bring this action pursuant to §§ 2511 and 2520 of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2511 and 2520, § 1030 of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, § 2701 of the Stored Communication Act ("SCA"), 18 U.S.C. § 2701, § 1983 of the Civil Rights Act, 42 U.S.C. § 1983, The Fourth Amendment of the United States Constitution, U.S. CONST. amend. IV, the Pennsylvania Wiretapping and Electronic Surveillance Act, 18 Pa. C.S.A. § 5701 *et seq.* ("PWESA"), and Pennsylvania common law.

4. This Court has original jurisdiction over Plaintiffs' and the Class' federal law claims pursuant to 28 U.S.C. §§ 1331 and 1137, and supplemental jurisdiction over Plaintiffs' and the Class' state law claims pursuant to 28 U.S.C. § 1367.

5. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391(b) and (c) as each Defendant is a resident of and/or maintains a permanent business office in this district.

6. In connection with the acts and conduct complained of, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including the internet.

THE PARTIES

7. Minor Plaintiff, Blake J. Robbins, is a high school student attending Harriton High School at 600 North Ithan Avenue, Rosemont, Pennsylvania, 19010. Harriton High School is part of the Lower Merion School District.

8. Plaintiffs, Michael E. Robbins and Holly S. Robbins, husband and wife, are the parents and natural guardians of Blake. J. Robbins, with a residence address of 437 Hidden River Road, Penn Valley, Pennsylvania, 19072-1112. Blake J. Robbins, Michael E. Robbins and Holly S. Robbins are hereinafter collectively referred to as "Plaintiffs."

9. Defendant, Lower Merion School District ("School District"), is a municipal corporation body politic within the Commonwealth of Pennsylvania with a principal place of business at 301 East Montgomery Avenue, Ardmore, Pennsylvania, 19003.

10. Defendant, Board of Directors of the Lower Merion School District ("Board"), is comprised of a nine (9) member board elected locally to act as a corporate body in fulfilling the School District's and the Commonwealth of Pennsylvania's obligation to provide public education. The Board can be contacted through its secretary, Fran Keaveney, with an address of 301 East Montgomery Avenue, Ardmore, Pennsylvania, 19003.

11. Defendant, Superintendent of Schools Christopher W. McGinley ("McGinley"), is a School District Administrator appointed by the Board to supervise the day to day operation of the School District. As such he is responsible for the implementation of policies, procedures and practices instituted by the Board. The School District, the Board and McGinley are hereinafter collectively referred to as "Defendants."

CLASS ACTION ALLEGATIONS

12. Plaintiffs bring this action as a Class Action under Rules 23(a), 23(b)(1), 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of a Class consisting of Plaintiffs and all other students of Harriton High School and Lower Merion High School who have been issued by the School District a laptop computer equipped with a webcam, together with their families. Excluded from the Class are the Defendants herein, any subsidiary of any of the Defendants, any family members of the Defendants who attend either high school, all employees and directors of Defendants or any subsidiary, and their legal representatives, heirs, successors or assigns of any such excluded person or entity.

13. The Class is so numerous that joinder of all members is impracticable. The student body of both high schools within the School District consists of approximately 1,800 students. Additionally, the proposed Class includes each high school student's immediate family members.

14. Plaintiffs' claims are typical of the claims of the other members of the Class, as Plaintiffs and all other members were injured in exactly the same way – by the unauthorized, inappropriate and indiscriminant remote activation of a webcam contained within a laptop computer issued to students by the School District and the intentional interception of their private webcam images in violation of federal and state law as complained of herein.

15. Plaintiffs will fairly and adequately represent the interests of the Class and has retained counsel competent and experienced in Class Action litigation.

16. Plaintiffs have no interests that are contrary to or in conflict with those of the Class.

17. A Class Action is superior to other available methods for the fair and efficient adjudication of this controversy. Since the damage suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it virtually impossible for the Class members individually to seek redress for the unlawful conduct alleged.

18. Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a Class Action.

19. Common questions of law and fact exist as to all members of the Class and predominate over any questions effecting solely individual members of the Class. Among the questions of law and fact, common to the Class:

a. Whether Defendants' acts as alleged herein violated the ECPA, the CFAA, the SCA, § 1983, The Fourth Amendment of the United States Constitution, the PWESA or Pennsylvania common law;

b. Whether Defendants participated in and pursued the concerted action or common course of conduct complained of; and

c. Whether Plaintiffs and members of the Class have sustained compensable damages and, if so, the proper measure of such damages.

SUBSTANTATIVE ALLEGATIONS

20. In the Superintendent of Schools welcome address appearing on the Lower Merion School District website as of the date hereof the Superintendent states as follows:

> The District is also in the final stages of implementing a one to one laptop computer initiative at the High Schools. Thanks in part to State and Federal grants secured by our technology staff during the past few years, every high school student will have their own personal laptop-enabling an authentic mobile 21st Century learning environment. The initiative, which was launched with great success at Harriton last year, enhances opportunities for ongoing collaboration, and ensures that all students have 24/7 access to school based resources and the ability to seamlessly work on projects and research at school and at home. The result: more engaged, active learning and enhanced student achievement. While other districts are exploring ways to make these kinds of incentives possible, our programs are already in place, it is no accident that we arrived ahead of the curve; in Lower Merion, our responsibility is to lead.

21. As part of this initiative as indicated by the Superintendent, laptop computers equipped with webcams have been issued on a one to one basis to all high school students in the School District.

22. An examination of all of the written documentation accompanying the laptop, as well as any documentation appearing on any website or handed out to students or parents concerning the use of the laptop, reveals that no reference is made to the fact that the school district has the ability to remotely activate the embedded webcam at any time the school district wished to intercept images from that webcam of anyone or anything appearing in front of the camera at the time of the activation.

23. On November 11, 2009, Plaintiffs were for the first time informed of the above-mentioned capability and practice by the School District when Lindy Matsko ("Matsko), an Assistant Principal at Harriton High School, informed minor Plaintiff that the School District was of the belief that minor Plaintiff was engaged in improper behavior in his home, and cited as evidence a photograph from the webcam embedded in minor Plaintiff's personal laptop issued by the School District.

24. Michael Robbins thereafter verified, through Ms. Matsko, that the School District in fact has the ability to remotely activate the webcam contained in a students' personal laptop computer issued by the School District at any time it chose and to view and capture whatever images were in front of the webcam, all without the knowledge, permission or authorization of any persons then and there using the laptop computer.

25. Additionally, by virtue of the fact that the webcam can be remotely activated at any time by the School District, the webcam will capture anything happening in the room in which the laptop computer is located, regardless of whether the student is sitting at the computer and using it.

26. Defendants have never disclosed either to the Plaintiffs or to the Class members that the School District has the ability to capture webcam images from any location in which the personal laptop computer was kept.

COUNT I – INTERCEPTION OF ELECTRONIC COMMUNICATIONS UNDER THE ECPA

27. Plaintiffs repeat and re-allege each and every allegation above as if fully set forth herein.

28. Plaintiffs and the Class assert this Count against all Defendants, jointly and severally, pursuant to §§ 2511 and 2520 of the ECPA, 18 U.S.C. §§ 2511 and 2520.

29. Section 2511 of the ECPA provides in part:

> (1) Except as otherwise specifically provided in this chapter any person who—
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept, or endeavor to intercept, any . . . electronic communications;
>
> * * * * *

(d) intentionally uses, or endeavors to use, the contents of any . . . electronic communication knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of this subsection; . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

30. Section 2520 of the ECPA provides in part:

(a) In general. –Except as provided in section 2511 (2)(a)(ii), any person whose . . . electronic communication is intercepted . . . or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) Relief.—In the action under this section, appropriate relief includes –

(1) such preliminary and other equitable or declaratory relief as may be appropriate

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

31. Section 2510 of the ECPA, setting forth the definitions of the terms in § 2511, defines "person" to include "any employee, or agent of the United States or any State or political subdivision thereof. . . ." 18 U.S.C. § 2510(6). Accordingly, each Defendant is a "person" within the meaning of § 2511.

32. Section 2510 defines "electronic communication" to include "any transfer of signs, signals, writing, imaging, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce, . . ." 18 U.S.C. § 2510(12). Accordingly, the webcam images complained of constitute an "electronic communication" within the meaning of § 2511.

33. Section 2510 defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Section 2510 defines "electronic, mechanical, or other device" to mean "any device or apparatus which can be used to intercept a wire, oral, or electronic communication," subject to exclusions not relevant to this action. 18 U.S.C. § 2510(5).

34. The software/hardware used by the School District to remotely activate the webcams complained of constitute an "electronic . . . device" within the meaning of 18 U.S.C. § 2510(5). By using said software/hardware to secretly obtain webcam images, each Defendant "intercepts" that communication within the meaning of § 2511.

35. By virtue of the foregoing, Plaintiffs and each member of the Class is a "person whose . . . electronic communication is intercepted...or intentionally used in violation of this chapter" within the meaning of § 2520.

36. By virtue of the foregoing, Defendants are liable to Plaintiffs and the other members of the Class for their violations of §§ 2511 and 2520 of the ECPA.

37. Since Plaintiffs first learned of Defendants' unlawful remote activation of the webcams complained of on November 11, 2009, this action is timely and not beyond ECPA's applicable statue of limitations.

38. Defendants' actions complained of herein were conscious, intentional, wanton and malicious, entitling Plaintiffs and the other members of the Class to an award of punitive damages.

39. Plaintiffs and the other members of the Class have no adequate remedy at law for Defendants continued violation of the ECPA.

COUNT II – THEFT OF INTELLECTUAL PROPERTY UNDER THE CFAA

40. Plaintiffs repeat and re-allege each and every preceding allegation as if fully set forth herein.

41. Plaintiffs and the Class assert this Count against Defendants, jointly and severally, pursuant to § 1030 of the CFAA, 18 U.S.C. § 1030.

42. Section 1030 provides in part:

> (a) Whoever-
>
> * * * * *
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (C) information from any protected computer if the conduct involved an interstate or foreign communication;
>
> * * * * *
>
> shall be punished as provided in subsection (c) of this section.
>
> (b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
>
> * * * * *
>
> (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. . . . No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

43. Section 1030 of the CFAA defines the term "protected computer" to include "a computer . . . which is used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). Each laptop issued by the School District and equipped with a webcam is used

in interstate communications and is therefore a "protected computer" within the meaning of § 1030.

44. Section 1030 of the CFAA defines the term "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). By using software/hardware to remotely activate the webcams complained of and intercept their images, each Defendant has gained "access a computer without authorization or exceeds authorized access" within the meaning of § 1030.

45. By virtue of the foregoing, Defendants are liable to Plaintiffs and the Class for their violations of § 1030 of the CFAA.

46. Since Plaintiffs first learned of Defendants remote activation of the webcams complained of on November 11, 2009, this action is timely as to Plaintiffs and each member of the Class.

47. Defendants actions complained of herein were conscious, intentional, wanton and malicious entitling Plaintiffs and other members of the Class to an award of punitive damages.

48. Plaintiffs and the other members of the Class have no adequate remedy of law for Defendants continued violation of the CFAA.

COUNT III – STORED COMMUNICATIONS ACT (18 U.S.C. § 2701)

49. Plaintiffs repeat and re-allege each and every preceding allegation as if fully set forth herein.

50. Section 2701 of the SCA provides, in pertinent part:

Except as provided in subsection (c) of this section, whoever-

> 1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> 2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

51. Section 2711 of the SCA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce. . . ." 18 U.S.C. §§ 2711, 2510(12). Accordingly, the webcam images complained of are "electronic communications" within the meaning of the SCA.

52. Section 2711 of the SCA defines "person" to include "any employee, or agent of the United States or of a State or political subdivision thereof, and any individual, partnership, association. . . ." 18 U.S.C. §§ 2711, 2510(6). Accordingly, all Defendants are "persons" within the meaning of the SCA.

53. Section 2711 of the SCA defines "electronic storage" to include "any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof. . . ." 18 U.S.C. §§ 2711, 2510(17)(A).

54. Defendants' use of the software/hardware to remotely activate the webcams complained of and to obtain their images constitutes an unauthorized acquisition of stored electronic communications in violation of the SCA.

55. Section 2701(b) of the SCA provides punishment in those instances where the unauthorized acquisition of stored electronic communications was not done for commercial gain

or advantage of "a fine under this title or imprisonment for not more than six months, or both. . . ." 18 U.S.C. § 2701(b)(B).

COUNT IV – VIOLATION OF THE
CIVIL RIGHTS ACT (42 U.S.C. § 1983)

56. Plaintiffs repeat and re-allege each and every allegation set forth above as if fully set forth herein.

57. Section 1983 states in pertinent part:

> Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity or other proper proceeding for redress. . . ."

58. All Defendants are "persons" within the meaning of § 1983, in that at all times material hereto they were acting under the color of state law as a political subdivision of the Commonwealth of Pennsylvania, or a representative thereof.

59. Defendants' clandestine remote activation of the webcams complained of deprived Plaintiffs and all members of the Class of their right to privacy as protected by the Fourth Amendment of the United States Constitution.

60. As Plaintiffs first learned of Defendants unlawful deprivation of their privacy rights on November 11, 2009, this action has been commenced within § 1983's applicable two-year statute of limitations.

61. Defendants' conduct in remotely activating the webcams complained of, which resulted in the deprivation of Plaintiffs' and the Class members' constitutionally-protected right

to privacy was intentional, extreme and outrageous, and thereby entitles Plaintiffs and the Class to an award of punitive damages.

COUNT V – INVASION OF PRIVACY (U.S. CONST. AMEND. IV)

62. Plaintiffs repeat and re-allege each and every preceding allegation as if fully set forth herein.

63. At a minimum, and pursuant to the Fourth Amendment of the United States Constitution, U.S. CONST. amend. IV, Plaintiffs and Class members had a reasonable expectation of privacy with respect to the use of the webcams embedded in the laptop computers issued by the School District.

64. In particular, Plaintiffs and Class members were never informed that the webcam incorporated into the students' personal laptop computer could be remotely activated by the School District and/or its agents, servants, workers or employees indiscriminately at the whim of the School District, and that such activation would naturally capture images of anything in front of the webcam at the time of its activation.

65. In as much as the personal laptop computers were used by students of the high schools and their families, it is believed and therefore averred that the School District has the ability to and has captured images of Plaintiffs and Class members without their permission and authorization, all of which is embarrassing and humiliating.

66. As the laptops at issue were routinely used by students and family members while at home, it is believed and therefore averred that many of the images captured and intercepted may consist of images of minors and their parents or friends in compromising or embarrassing positions, including, but not limited to, in various stages of dress or undress.

COUNT VI – PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE ACT (18 PA. C.S.A. § 5101, *ET SEQ.*)

67. Plaintiffs repeat and re-allege each and every preceding allegation as if fully set forth herein.

68. Section 5703 of the PWESA states in pertinent part:

> Except as otherwise provided in this chapter, a person is guilty of a felony of the third degree if he:
>
> 1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or aural communication;

69. Section 5702 of the PWESA defines "intercept" to include the "aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. C.S.A. § 5702.

70. Section 5702 of the PWESA defines "electronic communications" to include "any transfer of signs, signals, writing, images, . . . transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system. . . ." 18 Pa. C.S.A. § 5702.

71. Section 5702 of the PWESA defines "person" as "any employee, or agents of the United States or any state or political subdivision thereof. . . ." 18 Pa. C.S.A. § 5702.

72. Pursuant to § 5702 of the PWESA, Defendants are "persons" within the meaning of the Act, and Defendants' conduct with respect to the webcams complained of constitutes an interception of electronic communications violative of the PWESA.

73. Pursuant to § 5725 of the PWESA:

> Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication; and shall be entitled to recover from any such person:

1) Actual damages, but not less than liquidated damages computed at the rate of $100.00 a day for each day of violation, or $1,000.00, whichever is higher.

2) Punitive damages.

3) A reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT VII – INVASION OF PRIVACY: PENNSYLVANIA COMMON LAW[1]

74. Plaintiffs repeat and re-allege each and every preceding allegation as if fully set forth herein.

75. At all times material hereto, and pursuant to the common law of Pennsylvania, Plaintiffs and all members of the Class had a reasonable expectation of privacy with respect to the operation of the webcams complained of.

76. Plaintiffs and Class members were never informed of the School District's capability and practice of remotely activating the webcams complained of.

77. As the laptops at issue were routinely used by the students, their friends and family members while at home, it is believed and therefore averred that many of the webcam images captured and/or intercepted consist of minors and/or their parents in compromising or embarrassing positions, including, but not limited to, in various stages of dress or undress.

WHEREFORE, Plaintiffs, Blake J. Robbins, Michael E. Robbins, Holly S. Robbins and all members of the Class, request judgment in their favor and against Defendants, Lower Merion School District, The Board of Directors of the Lower Merion School District and Christopher W. McGinley, jointly and severally, as follows:

1) for compensatory damages;

[1] Should discovery disclose that Defendants are in possession of images constituting child pornography within the meaning of 18 Pa. C.S.A. §6312, *et. seq.*, Plaintiffs will amend this Complaint to assert a cause of action thereunder.

2) for punitive damages;

3) for liquidated damages pursuant to the PWESA;

4) for attorneys' fees and costs;

5) for declaratory and injunctive relief; and

6) for such other and further relief as this Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues for which a right to jury trial exists.

LAMM RUBENSTONE LLC

By: _____

Mark S. Haltzman, Esquire (#38957)
Stephen Levin, Esquire (#19300)
Frank Schwartz, Esquire (#52729)
3600 Horizon Boulevard, Suite 200
Trevose, PA 19053-4900
(215) 638-9330 / (215) 638-2867 Fax
Attorneys for **Plaintiffs and the Class**

DATED: February 11, 2010

IN THE SUPREME COURT OF THE UNITED STATES

- - - - - - - - - - - - - - - - - - x

CITY OF ONTARIO, CALIFORNIA, :

ET AL., :

Petitioners : No. 08-1332

v. :

JEFF QUON, ET AL. :

- - - - - - - - - - - - - - - - - - x

Washington, D.C.

Monday, April 19, 2010

The above-entitled matter came on for oral argument before the Supreme Court of the United States at 11:06 a.m.

APPEARANCES:

KENT L. RICHLAND, ESQ., Los Angeles, California; on behalf of Petitioners.

NEAL K. KATYAL, ESQ., Deputy Solicitor General, Department of Justice, Washington, D.C.; on behalf of the United States, as amicus curiae, supporting Petitioners.

DIETER DAMMEIER, ESQ., Upland, California; on behalf of Respondents.

C O N T E N T S

P R O C E E D I N G S

(11:06 a.m.)

CHIEF JUSTICE ROBERTS: We will hear argument next in Case 08-1332, the City of Ontario v. Quon.

Mr. Richland.

ORAL ARGUMENT OF KENT L. RICHLAND

ON BEHALF OF THE PETITIONERS

MR. RICHLAND: Mr. Chief Justice, and may it please the Court:

Under the less restrictive constitutional standards applied when government acts as employer, as opposed to sovereign, there was no Fourth Amendment violation here.

First, Ontario Police Sergeant Jeff Quon had no reasonable expectation of privacy vis-à-vis the Ontario Police Department in text messages on his department-issued pager in light of the operational realities of his workplace, which included the explicit no privacy in text messages policy.

CHIEF JUSTICE ROBERTS: The written policy?

(Laughter.)

CHIEF JUSTICE ROBERTS: The whole -- the argument here, of course, is that that was modified by the instructions he got from the lieutenant. Do we

1 follow the written policy or the policy they allegedly
2 enforced in practice?
3 MR. RICHLAND: That is the argument,
4 Mr. Chief Justice. But, in fact, there was no
5 inconsistency between the no privacy in text messages
6 aspect of the written policy and the oral information
7 he was given.
8 First of all, the written policy itself was
9 broad enough to cover text messages. It stated, for
10 example, at Appendix 152, that it applied to city-owned
11 computers and all associated equipment. And again at
12 152: "City-owned computer equipment, computer
13 peripheral, city networks, the Internet, e-mail, or
14 other city-related computer services." And, finally, the
15 agreement to the policy was that it applied -- this is
16 at Appendix 156 -- to city-owned computers and related
17 equipment.
18 So certainly the written policy itself was
19 broad enough to cover text messaging pagers, but in
20 addition to that, nothing in the oral statements made by
21 Lieutenant Duke undermined the no-privacy aspect of the
22 written policy.
23 CHIEF JUSTICE ROBERTS: Well, we are dealing
24 with Mr. Quon's reasonable expectations, right?
25 MR. RICHLAND: Yes, yes.

CHIEF JUSTICE ROBERTS: And even with the written policy, he has the instructions -- everybody agrees -- you can use this pager for private communications.

MR. RICHLAND: That’s correct.

CHIEF JUSTICE ROBERTS: We’re not going to audit them. Right? That's what he said. He has to pay for them. Right? Now, most things, if you're paying for them, they’re yours. And this -- it particularly covered messages off-duty.

Now, can't you sort of put all those together and say that it would be reasonable for him to assume that private messages were his business? They said he can do it. They said, you’ve got to pay for it. He used it off duty. They said they’re not going to audit it.

MR. RICHLAND: Not when he was told at the same time that these text messages were considered e-mail and could be audited, and that they were considered public records and could be audited at any time; that is, it has to do with a different aspect of what the policy -- the oral policy --

JUSTICE GINSBURG: In addition to -- that was said at the meeting -- and Lieutenant Duke, who was the same one who later says: I'm not going to monitor

as long as you pay the difference. There was the statement at the meeting by that same person. Wasn't there something in writing by the police chief to follow up after that meeting?

MR. RICHLAND: Yes, there was, Justice Ginsburg. There was a memo that was sent that memorialized the statements at the meeting, that specifically stated that the text messages were treated as e-mail under the written policy.

CHIEF JUSTICE ROBERTS: Let me ask you --

JUSTICE SOTOMAYOR: Counsel --

CHIEF JUSTICE ROBERTS: Let me ask you to put the written policy aside. Hypothetical case: There’s no written policy. Would he have a reasonable expectation in the privacy of his personal e-mail, text messages, in that case?

MR. RICHLAND: Not --

CHIEF JUSTICE ROBERTS: In other words, all we know is the list that I went through earlier.

MR. RICHLAND: Yes. Yes, Mr. Chief Justice. Assuming all the other factors in this case were present --

CHIEF JUSTICE ROBERTS: Yes.

MR. RICHLAND: That is, he is using his department-issued pager; he is a police officer and

indeed a member of the high-profile SWAT team of the police department. He should be aware just by virtue of that fact that there is going to be litigation involving incidents that the SWAT team gets involved in where there will be requests for the communications that are made on that official department-issued pager.

And, in addition, he should be aware of the fact -- and this is something that the dissenters to denial of en banc said below. He should be aware that there may be inquiries from boards of the police to determine whether the conduct of the police in a particular incident is appropriate.

JUSTICE SCALIA: Mr. Richland, a little earlier you referred us to page 152 and 156 of --

MR. RICHLAND: Of the appendix to the petition.

JUSTICE SCALIA: Oh, the appendix to the petition.

MR. RICHLAND: Yes, and that's the policy. That is the written policy, Justice Scalia. I'm sorry for the confusion.

CHIEF JUSTICE ROBERTS: Well, that’s the written policy.

MR. RICHLAND: That is the written policy, and the --

CHIEF JUSTICE ROBERTS: But the policy itself, from the point of view of Officer Quon, is a little bit more complicated than that.

MR. RICHLAND: Well, of course, what the -- what Officer Quon's point of view is must also be tempered by what we are reasonably going to accept as a society of his understanding of the circumstances.

JUSTICE SOTOMAYOR: Counsel --

CHIEF JUSTICE ROBERTS: You would agree, I think, that if the SCA, the Stored Communications Act --

MR. RICHLAND: Yes.

CHIEF JUSTICE ROBERTS: If that made it illegal to disclose these e-mails, then he would certainly be correct that he has a reasonable expectation of privacy; isn't that right?

MR. RICHLAND: No, Mr. Chief Justice. We would not agree with that.

CHIEF JUSTICE ROBERTS: It's not reasonable to assume that people are going to follow the law?

MR. RICHLAND: Well, for several reasons. Number one, this Court has repeatedly stated that the mere fact that something is contrary to the law does not in itself permit a reasonable expectation of privacy. Just two terms ago, in Virginia v. Moore, this Court said precisely that. And of course it said it earlier

in California v. Greenwood, and in a number of other cases -- Oliver v. United States.

Because the effect of that, of course, would mean that we would be constitutionalizing every positive law that might be enacted by a State or the Federal legislature.

JUSTICE KENNEDY: Well, on that point, do we take it as the law of the case or as a given that it was illegal for I think Arch to turn over the transcripts to the police department? What do we do with that part of the case?

MR. RICHLAND: Justice Kennedy, I don’t believe it is law of the case that is binding on this Court, since this Court is a higher court. Although it is true that this Court denied certiorari on that issue, I don't believe it is bound by the Ninth Circuit determination of that, and in fact it is our contention that that was incorrectly decided.

JUSTICE KENNEDY: On remand -- has there been a final judgment issued as to Arch, or is that just being held --

MR. RICHLAND: I don't believe so, Justice Kennedy. I believe that everything has been stayed pending the determination by this Court.

JUSTICE SOTOMAYOR: Counsel, let's assume

that in this police department, everyone knew, the supervisors and everyone else, that the police department people spoke to their girlfriends at night.

MR. RICHLAND: Yes, Justice Sotomayor.

JUSTICE SOTOMAYOR: And one of the chiefs, out of salacious interest, decides: I'm going to just go in and get those texts, those messages, because I just have a prurient interest. Does that officer have any expectation of privacy that his boss won't just listen in out of prurient interest?

MR. RICHLAND: Justice Sotomayor, as to the first aspect, the question of reasonable expectation of privacy, the motive should have no impact. The motive of looking should have no impact. The question of reasonable expectation of privacy must be analyzed according to the relationship between the officer and his -- and his employer.

JUSTICE SOTOMAYOR: But if in fact -- and whether we agree with this conclusion or not, we accept the lower court's views that there was an expectation that the chiefs were not going to read these things, some expectation of privacy --

MR. RICHLAND: Yes.

JUSTICE SOTOMAYOR: -- the limits of it have to be limited for all of the reasons you've said, doesn't

this case begin and end on whether or not what the jury found is reasonable grounds for what the city did?

MR. RICHLAND: I think that what this case begins and ends with, if we assume that there was a reasonable expectation of privacy, is under the plurality opinion in O'Connor: Whether the search itself was reasonable. And the jury did, of course, make a determination as to the purpose of the search.

JUSTICE SCALIA: I guess we don't decide our -- our Fourth Amendment privacy cases on the basis of whether there -- there was an absolute guarantee of privacy from everybody. I think -- I think those cases say that if you think it can be made public by anybody, you don't -- you don't really have a right of privacy.

So when the -- when the filthy-minded police chief listens in, it's a very bad thing, but it's not -- it’s not offending your right of privacy. You expected somebody else could listen in, if not him.

MR. RICHLAND: I think that's correct, Justice Scalia.

JUSTICE SCALIA: I think it is.

MR. RICHLAND: And I think the reason why you must have the two-step analysis in a case of this sort -- that is, first look at the question as to whether there’s a reasonable expectation of privacy,

and then determine, if there was, whether the search was reasonable -- is precisely for the reason that, without that, what we will have in every case is the claim that there was a salacious reason, that that was the reason. And we'll be litigating every one of those cases --

JUSTICE GINSBURG: Then, according to what you just said, the jury determination was superfluous. If there was no reasonable expectation of privacy because the officers were told this is just -- we treat this just like e-mails, it can be monitored, it can be made public, then there would be no reasonable expectation of privacy and there would be no question to go to the jury.

MR. RICHLAND: That's correct, Justice Ginsburg. And it is our position that this should never have gone to the jury, that summary judgment should have been granted in favor of the Ontario Police Department.

JUSTICE KENNEDY: So you have two arguments: One, that it's -- there's no reasonable expectation of privacy; even if there were, that this was a reasonable search.

MR. RICHLAND: That's correct.

JUSTICE SCALIA: Is reasonable expectation of privacy a judge question or a jury question?

MR. RICHLAND: Well, if there is a conflict in the facts, I presume the jury must resolve those -- that factual conflict. But in this case, I don't believe there is a conflict in the facts, and, therefore, it is a judge question.

CHIEF JUSTICE ROBERTS: Did your client treat on-duty text messages different from off-duty text messages?

MR. RICHLAND: It did, once there was an initial determination made as to the --

CHIEF JUSTICE ROBERTS: Why did it do that?

MR. RICHLAND: Excuse me. I'm sorry.

CHIEF JUSTICE ROBERTS: Why did it treat them differently? Under your theory, they're all the same -- no expectation of privacy.

MR. RICHLAND: It treated them differently out of -- because there were two aspects to the case. One aspect was the initial determination that Chief Sharp ordered to say: I just want to know, is our character limit efficacious here, or do we need to have a higher character limit? And for that purpose, they needed to just look at all of them. And they did; they looked at all of the text messages.

But then when they saw that some of them may have involved violations of department regulations, then

it was sent to Internal Affairs, and they redacted the off-duty messages because they were --

JUSTICE KENNEDY: Is that something like the plain view argument? In search and -- search and --

MR. RICHLAND: I suppose.

JUSTICE KENNEDY: Well, I'm serious. In other words, there is, under your view --

MR. RICHLAND: Yes.

JUSTICE KENNEDY: -- legitimate grounds to look at the messages, and then once they see it, they don't have to ignore it.

MR. RICHLAND: I think that’s correct, Justice Kennedy.

CHIEF JUSTICE ROBERTS: Well, why did -- I'm sorry. I still don't understand. It redacted them, right?

MR. RICHLAND: Redacted because the inquiry -- the second stage of the inquiry in Internal Affairs --

CHIEF JUSTICE ROBERTS: Yes.

MR. RICHLAND: -- was simply to determine how much time was being spent on duty sending personal messages.

CHIEF JUSTICE ROBERTS: Right.

MR. RICHLAND: So the Internal Affairs Department said: We don't need to look at the off-duty messages. We’re going to redact them. Why get into all

of that? We don't have to look.

The department was pretty scrupulous. And I think that's part of what makes the entire approach that they took to this reasonable. It makes the search aspect of the case reasonable. And I think it's important, in that regard, to look at the nature --

JUSTICE SCALIA: Excuse me. You said they did get to the off-duty text messaging later?

MR. RICHLAND: No, it was the other way around. They looked at the on-duty text messaging at the later stage, at the Internal Affairs stage. But they looked at all of the text messages when the only purpose for the inquiry was to determine how many of the text messages in general are job-related and how many were personal? Because the question was: Do we need to raise the character limit --

CHIEF JUSTICE ROBERTS: Well, you don't have to look at the messages to determine that with respect to the off-duty messages, right?

MR. RICHLAND: Well -- well, you did, because of the fact, Mr. Chief Justice, that there were job-related communications even while there was off-duty. These officers were SWAT team officers. They were on duty, as Sergeant Quon said, 24/7. That was one of the reasons why they had the text messaging pagers.

JUSTICE ALITO: If someone wanted to send a message to one of these pagers, what sort of a device would you need? Do you need to have another pager, or can you -- could you send a message to one of these devices from some other type of device?

MR. RICHLAND: No, there were messages that were sent from various other devices. Is the question whether that could be physically done, electronically done? Because, yes, clearly that was --

JUSTICE ALITO: Yes. What other type of device could you use to send a message to one of these pagers?

MR. RICHLAND: It -- oh. I'm not certain if it was something other than another text messaging pager. It did appear that there were some e-mail entries in the transcripts themselves, which suggested that there might have been a way to communicate to them with e-mail, but that's just -- that's all in the record that suggests that.

JUSTICE SCALIA: You know, if they were on duty 24/7, there weren't any off-duty messages, were there?

(Laughter.)

MR. RICHLAND: Well, I may have misspoke. They were on call 24/7. They were the SWAT team, and

1 they had to respond to emergencies.

2 JUSTICE GINSBURG: If we take it that the

3 Stored Communications Act does say that the provider may

4 not give out the transcripts, if we take that as given,

5 then how can the department lawfully use the

6 transcripts?

7 MR. RICHLAND: Well, Justice Ginsburg, first

8 of all, there was no -- there is no current claim that

9 anything that the department did with respect to the

10 Stored Communications Act was unlawful. So it may be

11 that the other entity, Arch Wireless, violated the

12 Stored Communications Act, but that would not preclude

13 the department -- which was, after all, the subscriber

14 -- from requesting to see what, in fact, the transcripts

15 disclosed.

16 But in addition to that, there is also the

17 fact that, as I said before, a reasonable expectation of

18 privacy couldn't be based simply on the fact that there

19 was a statute, and particularly not a statute like the

20 Stored Communications Act, because that's a statute that’s

21 extremely, extremely technical. And there is a --

22 one has to determine whether an entity was working

23 either as an electronic communications service or a

24 remote computing service, and so on. Courts are all

25 over the board on this. As this Court noted in United

States v. Payner, a complicated law like that simply cannot be the basis for a reasonable expectation of privacy.

And if I may reserve the rest of my time, thank you.

CHIEF JUSTICE ROBERTS: Certainly, counsel.

Mr. Katyal.

ORAL ARGUMENT OF NEAL K. KATYAL,

ON BEHALF OF THE UNITED STATES, AS AMICUS CURIAE,

SUPPORTING THE PETITIONERS

MR. KATYAL: Thank you, Mr. Chief Justice, and may it please the Court:

Millions of employees today use technologies of their -- of their employers under policies established by those employers. When a government employer has a no-privacy policy in place that governs the use of those technologies, ad hoc statements by a non-policy member cannot create a reasonable expectation of privacy. Put most simply, the computer help desk cannot supplant the chief's desk. That simple, clear rule should have decided this case.

Instead, the Ninth Circuit found that the 1999 policy applied to pagers, but then concluded that that 1999 policy was informally modified years later. And that decision should be reversed. It disregards

1 this Court's repeated holdings, including 2 years ago in
2 the Chief Justice's opinion in Engquist v. Oregon about
3 the greater amount of leeway that the government has
4 when it acts as an employer. And it also is not
5 consistent with the plurality opinion in O'Connor, which
6 observed that when the government adopts a policy that
7 its employees lack privacy, no reasonable expectation of
8 privacy exists.
9 JUSTICE KENNEDY: Let me ask you this:
10 Suppose the department asks for opinion of legal
11 counsel whether or not transmittal of the transcripts by
12 Arch to the department was a violation of the Act, and
13 the counsel said: This was a violation of the Act; they
14 had no right to send them to you. Would the department
15 then still have had a right to look at the transcripts?
16 MR. KATYAL: So the question is if the
17 Stored Communications Act is violated?
18 JUSTICE KENNEDY: Yes. Yes.
19 MR. KATYAL: We don't think the Stored
20 Communications Act was --
21 JUSTICE KENNEDY: No, but -- no, my
22 hypothetical is that the -- that there is a legal
23 counsel's opinion that this was in violation of the Act,
24 and let's say the district court said it is in violation
25 of the Act. Let's say we say it’s in violation of the

Act. Is that the end of case? The department cannot look at the transcripts?

MR. KATYAL: Oh, absolutely not. I mean, I think this Court has repeatedly said that -- that various privacy laws don't determine the scope of the Fourth Amendment. I think it said so most clearly in California v. Greenwood. And I think that's for a very simple reason, that things like the Stored Communications Act, Justice Kennedy, the Electronic Communications Privacy Act, came about --

JUSTICE KENNEDY: Well, California v. Greenwood was a question of -- of a Fourth Amendment standard that had to be nationwide. So you say it's the same -- same thing here?

MR. KATYAL: I -- I do think it’s the same, and for this simple reason, that when you have a nationwide standard or a State standard, it’s to fill the gap, whatever isn’t necessarily protected by the Fourth Amendment. And here --

JUSTICE KENNEDY: Well, but Greenwood was in the -- in the context of the exclusionary rule in criminal proceedings. I certainly think that States -- at least we could make the reasonable argument that States can have different policies with respect to their employees, that have to be respected.

MR. KATYAL: Absolutely, Justice Kennedy. I don't disagree with that. I think the only question is, if the -- if I understand your question it’s, does a Federal statute about privacy somehow matter to the Fourth Amendment analysis about reasonable expectations of privacy? And there our contention is, no; it’s precisely because Congress enacted the Stored Communications Act to fill gaps in Fourth Amendment law. That -- that's why it's enacted.

And for -- for this Court to then use that very Act to be the template on which reasonable expectations of privacy may spring I think would be a very -- it would be a novel proposition. Nor should --

JUSTICE ALITO: Well, that's -- that's a little bit puzzling because there are -- electronic communications are stored all over the place in -- and there isn't a history -- these are -- these are relatively new. There isn't a well-established understanding about what is private and what isn't private. It's a little different from putting garbage out in front of your house, which has happened for a long time.

If -- if statutes governing the privacy of that information don't have any bearing on reasonable expectation of privacy under the Fourth Amendment, it's

some -- I -- I'm at something of a loss to figure out how to determine whether there is a reasonable expectation of privacy regarding any of those things.

MR. KATYAL: Well, Justice Alito, I do think that the underlying premise of your question is one with which we entirely agree. These are technologies that are rapidly in flux, in which we don't have intuitive understandings the way we do about, say, trash and so on. And it's precisely for that reason I think the Court should be very careful to constitutionalize and generate Fourth Amendment rules in this area at the first instance.

To do so I think really does freeze into -- into -- into place something that the legislature can't then fix, going to Justice Kennedy's opinion in, for example, Murray v. Giarratano, in which he said that constitutionalizing in that area -- constitutionalizing may pretermit legislative solutions.

Now, here the Stored Communications Act is not violated under any way, shape, or form. The Stored Communications Act has two different provisions in it, one having to do with remote -- remote computing services, RCSs. That's when an entity offers storage facilities. And the other is for an electronic communications service. That is essentially transmission

of messages from point to point.

CHIEF JUSTICE ROBERTS: Your point that you made just a moment ago, that we don't want to freeze into place the constitutional requirements with respect to new technology, I wonder if it cuts the other way. We're dealing with an amendment that looks to whether something is reasonable. And I think it might be the better course to say that the Constitution applies, but we're going to be more flexible in determining what's reasonable because they are dealing with evolving technology.

MR. KATYAL: Well, I think that the -- the best way -- I think the most -- the easiest way for the Court to resolve this is to simply say that when we are dealing with what is reasonable, we look to the policy. And here there's a policy by the employer, it says that computer-associated -- computer-related equipment and others, there's no expectation of privacy. You have a person who is told that repeatedly.

CHIEF JUSTICE ROBERTS: Well, but that puts a lot of weight -- I mean, there are some things where we don't bind them. You know, you get the usual parking garage thing that has got all this small print on the back. We -- we don't say that you're bound by that, because nobody reads it.

But in here, I just don't know. I just don't know how you tell what's reasonable -- I suspect it might change with how old people are and how comfortable they are with the technology -- when you have all these different -- different factors.

You know, they're told you can use it for private; you've got to pay for it. I think if I pay for it, it's mine, and it's not the employer's.

MR. KATYAL: Well, I think the clearest way, Mr. Chief Justice, to decide what is reasonable and what isn't is actually the terms of the policy. And it seems to me very little is more unreasonable than expecting a right to privacy after you've been told in a policy you have no privacy.

JUSTICE SCALIA: Suppose we find a right of privacy. Is that the end of the case? I mean, wouldn't you also -- in order to sustain this lawsuit, wouldn't you also have to find that it was an unreasonable --

MR. KATYAL: Absolutely. There are two arrows in the city's quiver, and I think they're right as to both of them. But --

JUSTICE SCALIA: What's the government's position on the unreasonableness of the search?

MR. KATYAL: The government's position is that the Ninth Circuit just from the get-go got the

standard wrong by citing -- by using a Schowengerdt test which was, was this -- was this search the least restrictive alternative? And we think this Court has repeatedly said that's the wrong way of thinking about it, that that puts judges in the position of second-guessing searches on the ground, that they're not really fully -- fully equipped to do so.

So I do think that is a possible way to resolve this, Justice Scalia, but --

JUSTICE SCALIA: Maybe an easier way, huh?

MR. KATYAL: Well, I don't know that it's easier, in the following sense: I think that thousands of employers across the country rely on these policies and millions of employees. And the Ninth Circuit's decision puts that reliance in some jeopardy, because it said that you can have an official policy and it can be taken back by what some ad hoc subordinate says. And that is, I think, a very destructive notion to the idea of reliance on these policies and setting --

CHIEF JUSTICE ROBERTS: So, your -- your position would require people basically to have two of these things with them, two whatever they are, text messager or the BlackBerries or whatever, right? Because assuming they're going to get personal things, you know, some emergency at home, they're also going to

1 get work things --
2 MR. KATYAL: To the -- under this policy,
3 yes. You might have an employer that sets a different
4 policy and allows for some de minimis use and a zone of
5 privacy in that use. You can have a variety of
6 different things. But what I think would be dangerous
7 is to have a blanket rule that constitutionalizes and
8 says you always have reasonable expectations of privacy
9 in this technology. The result may be,
10 Mr. Chief Justice, that employers then won't give that
11 technology at all to their employees and -- and
12 eliminate even that de minimis use.
13 Mr. Chief Justice, you had also asked before
14 about the standpoint of Quon in -- in evaluating
15 the reasonableness of the search -- of the search in his
16 perspective of the policy. We think that is the wrong
17 way of looking at it. Instead, we think the proper test
18 is the written policy, what it says, and that is the
19 simplest way, I think, to provided administrability to
20 the lower courts. They can simply say was this policy
21 in existence, and not get into those questions of is it
22 like a parking ticket, did I flip through it too
23 quickly, did I understand that the policy and the like.
24 JUSTICE SOTOMAYOR: You want to -- you want
25 to -- you want to undo O'Connor's operational realities

of the workplace and say the minute you issued a written policy that renders all searches okay, even if the operational realities are different?

MR. KATYAL: Not at all, Justice Sotomayor. I take it the language about operational realities in the workplace, what is right next to it is looking to whether or not there are regulations in place, and here a policy is a regulation. And so --

JUSTICE SOTOMAYOR: You may have an argument that the nature of the policy here and all of the activities related to it don't prove an operational reality of privacy, but I don't know why -- you want a flat rule that says once you have a written policy, there’ no expectation of privacy.

MR. KATYAL: And I think that is -- that is what O'Connor says with respect to the -- as long as the policy is in place, that -- that's what O'Connor permits.

CHIEF JUSTICE ROBERTS: Thank you, counsel.

Mr. Dammeier.

ORAL ARGUMENT OF DIETER DAMMEIER

ON BEHALF OF THE RESPONDENTS

MR. DAMMEIER: Thank you, Mr. Chief Justice, and may it please the Court:

I think an underlying fact that we might be

skipping over is -- is -- and both the lower courts recognize this -- that the computer policy that the department had didn't apply to the pagers on its own. It -- it only came into play after Lieutenant Duke modified that policy and told people at the -- at the meeting that was referred to earlier that the pagers are now going to be applying with -- with this policy. It -- it --

JUSTICE GINSBURG: Why is -- why is that so? I mean, it did say associated equipment. And -- and if an employee is told now e-mails aren't private, so we're warning you, we can monitor them, wouldn't such an employee expect the same thing to apply to the pager?

MR. DAMMEIER: Well, the policy itself has two components to it. One is, don't use our equipment, all associated equipment for personal business.

The other part of that policy deals with the no privacy, and it informs the people there could be monitoring. And specifically on the acknowledgment form of that policy, which is at Appendix 156 of the petition, it specifically says the city will periodically monitor e-mail, Internet use, and computer usage.

And -- and, again, I think this is why the -- both lower courts came to the conclusion that the

1 computer policy on its own wasn't in play until
2 Lieutenant Duke announced that, hey, now the pagers are
3 going -- are going to be in play with this computer
4 policy. This is the same Lieutenant Duke --
5 JUSTICE GINSBURG: But my question is, an
6 employee reads this policy and says, oh, my e-mails are
7 going to be subject to being monitored --
8 MR. DAMMEIER: Sure.
9 JUSTICE GINSBURG: Wouldn't that employee
10 expect that the policy would carry over to pagers? I mean,
11 would -- when you think of what's the reason why they want
12 to look at the e-mails, wouldn't the same reason apply?
13 MR. DAMMEIER: Well, I'm sure the same
14 reasons could apply, but the -- the city is the one that
15 writes the rules here. The -- if they want to make it
16 clear on what it applies to, it certainly should be on
17 them to write them clear so the employee understands.
18 CHIEF JUSTICE ROBERTS: Maybe -- maybe
19 everybody else knows this, but what is the difference
20 between a pager and e-mail?
21 MR. DAMMEIER: Sure. The e-mail, looking at
22 the computer policy -- that goes through the city's
23 computer, it goes through the city's server, it goes
24 through all the equipment that -- that has -- that the
25 city can easily monitor. Here the pagers are a separate

device that goes home with you, that travels with you, that you can use on duty, off duty, and --

CHIEF JUSTICE ROBERTS: You can do that with e-mails.

MR. DAMMEIER: Certainly, certainly. But in this -- in this -- in this instance with the pagers, it went through no city equipment; it went through Arch Wireless and then was transmitted to another -- another person.

So, again, to Duke -- Duke is the one that said: Hey, this -- this comes into play. But Lieutenant Duke is also the one that gave the privacy guarantee to the SWAT team members and said: As long as you pay the overages, we’re not going to look at your pagers; we're not going to look at the messages. So if -- if you couple both of those modifications, both by the same lieutenant -- and he wasn't just some subordinate; he was the lieutenant in charge of the administrative bureau; he was the administrative bureau commander.

JUSTICE GINSBURG: I thought that he said -- he was saying: But as far as billing is concerned, I'm not going to look at these; if you use more than 25,000 characters, you pay the extra, and that will be the end of it. If you contest that, then I’ll look to see whether those in excess of 25,000 characters were for

work purposes or private purposes.

And so he's talking about the billing. He hasn't retracted what was said at the meeting about -- that these text messages are subject to audit.

MR. DAMMEIER: This -- this is what Sergeant Quon testified to, that he attributed to Lieutenant Duke: If you don't want us to read it, pay the overage fee.

JUSTICE BREYER: But what’s wrong with his deciding: I don't like to do this anymore? I don't want to collect all this money; it's too complicated; and so I don't know how many of these messages are related to work and how many they are just mucking around prying into each other's business.

MR. DAMMEIER: He can certainly --

JUSTICE BREYER: So I would like to know, so therefore I'm going to look and see. Now, what’s unreasonable about that?

MR. DAMMEIER: Well, he certainly could say I don't want to do this anymore, and he could --

JUSTICE BREYER: Oh, no.

MR. DAMMEIER: And he could tell everybody.

JUSTICE BREYER: I'm saying what's -- the city owns the pager. It's a pager used for work. They are giving a privilege to people if they want to

use it off work. It seems to be involving a big amount of collection, and so what he wants to do is he wants to see how much of this is being used for work and how much is of this not being used for work.

My question, which I just repeated, is why is that an unreasonable thing?

MR. DAMMEIER: I don't think that request is unreasonable, Your Honor.

JUSTICE BREYER: Fine. And then if that’s not unreasonable, why is what went on here that is any different?

MR. DAMMEIER: Well, here the jury -- the only fact that was determined by the jury was the reason for the search. And that's found at the appendix to the petition page 119. This is the only finding that the jury made as to the purpose of the search: To determine the efficacy of the existing character limits to ensure that officers were not being required to pay for the work-related expenses.

JUSTICE BREYER: How does that differ from what I just said?

MR. DAMMEIER: Well, it -- it comes into play on -- on the scope of the search. Again --

JUSTICE BREYER: No, I understand. I thought it's just a more -- a few more words to say just what I

said. That they wanted to look into this because they are tired about collecting so much money.

It's the third time I've said the same thing; probably it's my fault I'm not being clear. But it looked as if they wanted to know how many are being sent for work purposes, how many for private purposes including prying into people's business, which wasn't too desirable, and -- and -- so that they could get the -- the charges right.

Now, that sounds like what the jury said they were doing, too. And my question was -- I don't see anything, quite honestly, unreasonable about that, where you're the employer, where it's a SWAT team, where -- where -- where you're paying for this in the first place. So the reason I ask it is I would like you clearly to explain what's unreasonable about it.

MR. DAMMEIER: The scope of the search was unreasonable.

JUSTICE BREYER: That's the conclusion. Now, what's your reason?

MR. DAMMEIER: Under -- under -- looking at O'Connor, you have to -- you have to look to make sure that the search is not excessively intrusive. Here, what they did was they took all the messages and started reading them. Given the purpose, the limited purpose

that was found by the jury for the search, they didn't need to do that.

JUSTICE BREYER: Well, explain that one to me.

MR. DAMMEIER: They --

JUSTICE BREYER: Being naive about this, if I had a -- like, 20, 30,000 characters in 1,800 messages and I wanted to know which are personal and which are work-related, a good way to get at least a good first cut would be to read them.

(Laughter.)

JUSTICE BREYER: Okay? So I start off thinking that seems to be reasonable to me. That's what I would do.

MR. DAMMEIER: Well, that's certainly one --

JUSTICE BREYER: So all right. Now you tell me why that isn't reasonable.

MR. DAMMEIER: That's one of the ways they could have done it. They could have got -- they could have got consent from the officers first to do it. They could have had the officers themselves count the messages. After all, the officers were the ones that were paying for the overages.

JUSTICE BREYER: All right. But the officers might say: I don't want you to read these

messages because they happen to be about the sexual activity of some of my coworkers and their wives and me, which happened to be the case here.

MR. DAMMEIER: Right.

JUSTICE BREYER: So I guess if you had asked for consent, the officer would have said no.

(Laughter.)

JUSTICE BREYER: Now, he says, I still want to know. I will be repeating it. All right. So what -- that didn't sound very practical. What's the other way?

MR. DAMMEIER: Well, they could have -- they could have had the officers themselves count the messages.

JUSTICE BREYER: Well, the officer is going to say, hey, these are all big -- work-related. I'll tell you that. I only had two.

MR. DAMMEIER: Well --

(Laughter.)

JUSTICE BREYER: Okay. What's a third way?

MR. DAMMEIER: Okay. They -- the lieutenant could have said, hey, we're going to stop this practice that I started, and from this month forward make sure all you do is business-related. No more --

JUSTICE BREYER: That would have been rough on them. Because you want to let them have a few; you

need pizza when you're out on duty. You want to -- there are --

MR. DAMMEIER: The --

JUSTICE BREYER: Look, so far I listened to four things, and I'm just being naive about it. I'll read it more closely, but I don't see why these four things are so obviously more reasonable than what they did.

MR. DAMMEIER: They also -- they could have had the officers redact the private messages and then given it -- given it to the department.

JUSTICE SOTOMAYOR: But suppose that their application of what -- how much was being spent on business-related, all of your suggestions about having the officer do things does nothing about their application.

MR. DAMMEIER: Well --

JUSTICE SOTOMAYOR: You're -- you're relying on the very person you're auditing to do the audit for you. That doesn't seem either practical or business-wise.

MR. DAMMEIER: Well, other than my one sample of -- example of saying, hey, let's -- let's stop the personal use and we're going to have a test month to determine exactly how many messages we need for our business-related purposes.

JUSTICE SOTOMAYOR: That goes back to -- I

1 don't understand that. You're still relying on the
2 person you're auditing to say to you I'm only using
3 it for business. That -- that's just not logical.
4 MR. DAMMEIER: Well, but the -- the sole
5 purpose of the search was only to find out if officers
6 were paying for business-related messages that they
7 didn't need to pay for.
8 JUSTICE BREYER: But the question, in the
9 Constitution, the word is "unreasonable." Is it a
10 reasonable or unreasonable? So the question -- what I
11 asked is not maybe you would have gotten a better result
12 if you had hired Bain Associates and Bain would have
13 done a 4-month study at a cost of $50,000.
14 But I could say a person who doesn't want
15 to hire Bain and who doesn't want to rely on the
16 unverified word of the officers who were using these for
17 God knows what is not being unreasonable. That's the
18 ultimate issue. And that's why I'm putting it to you
19 to show me that what they did was unreasonable.
20 MR. DAMMEIER: I think it comes down from
21 that perspective on the excessiveness of the search.
22 CHIEF JUSTICE ROBERTS: The only reason --
23 the only reason the officer would not be accurate -- I
24 mean, I don't understand why the redaction is such a bad
25 idea. He just says these are private. And that allows

-- and then you could look at everything else. You can see if he's going too far because then everything else would be there. But in terms of -- the jury found this was not done to find out what was in the messages, so they don't need to find out what’s in the messages. That's just a question. He has to pay for everything he -- he redacts.

MR. DAMMEIER: That -- that's exactly what we’re saying. I mean, the interest here is -- is for the officer to be upfront as far as what’s business-related to -- if he's paying for things that he shouldn't be paying for, I'm sure he would -- he would be forthright about that.

CHIEF JUSTICE ROBERTS: I mean, it's no different than the police coming in and saying, well, we’re going to look at, you know, what's in every drawer and then -- you know, then if it turns out to be personal and private, we won't -- you know, we won't -- it just happens that we came upon, I guess, is Justice Kennedy's point. It's kind of the plain view doctrine, except they get to decide how broad what they can view is.

MR. DAMMEIER: That's true. I agree with that.

JUSTICE STEVENS: Can I ask you this question

about the basic background of a reasonable expectation of privacy? This is SWAT team work. Supposing it was an officer answering 911 calls or things like that. Isn't there sort of a background expectation that sooner or later, somebody might have to look at communications for this particular kind of law enforcement officer?

MR. DAMMEIER: Well, certainly -- certainly that could happen in any number of --

JUSTICE STEVENS: I mean, wouldn't you just assume that that whole universe of conversations by SWAT officers who are on duty 24/7 might well have to be reviewed by some member of the public or some of their superiors?

MR. DAMMEIER: But that -- that could be a possibility on any -- on anything that they do in their lives, whether it be their personal life or --

JUSTICE STEVENS: Well, but it's over official -- it's over the official communications equipment that they use for purposes of law enforcement.

MR. DAMMEIER: Correct. Correct.

JUSTICE KENNEDY: I certainly -- criminal defense attorneys challenging probable cause would want to look at these. They would want to see if there is exonerating evidence, under the rule that all exonerating evidence has to be submitted. It would seem

to me that it's quite likely, as Justice Stevens' question indicates, that there is going to -- that these are going to be discoverable.

MR. DAMMEIER: Well, it's just like my mail that I might send out to somebody. It might be discoverable in litigation, but that doesn't --

JUSTICE KENNEDY: But you're not -- you're not a police officer who is making arrests. I mean, this -- this is part and parcel of determining probable cause and mitigating evidence.

MR. DAMMEIER: No, it -- obviously, there are different reasons that could come into play that would legally produce these messages, certainly.

JUSTICE SCALIA: Mr. Dammeier, you could say the same thing about private phones. There are obviously circumstances in which whether you were making a call between certain times becomes relevant to litigation. So you could say that destroys the expectation of privacy? I'm not sure. I hope we don't say that.

MR. DAMMEIER: No. No. It's like -- this -- in O'Connor, all nine Justices in O'Connor found an expectation of privacy in Dr. Ortega's desk, because even though it was a state-owned desk, you still have an expectation of privacy.

JUSTICE STEVENS: Yes, but there’s no normal reason for going through somebody's desk; whereas, there would be a very ordinary -- ordinary reason for reviewing calls made to the SWAT -- members of the SWAT team, it seems to me.

MR. DAMMEIER: Well, there are -- as talked about in O'Connor, there are certainly a lot of valid reasons to go through a public employee's desk, if you’re looking for a file or if you’re looking for --

JUSTICE STEVENS: Yes.

MR. DAMMEIER: Or for -- or for an investigation. But still, there was that expectation of privacy. You’re talking about employees that -- in today's society, I think work and private life get melded together. Here, we’re talking about SWAT people 24/7 --

JUSTICE SCALIA: Well, to say that there’s an expectation of privacy in the desk doesn't say that every intrusion into that expectation of privacy is an unreasonable one. There could be that expectation of privacy and, still, for some reason -- let's assume there has been a theft in the building, and it's known that what was taken has not gotten out of the building. It's conceivable that that would be a valid reason to intrude upon the expectation of privacy, right?

MR. DAMMEIER: Correct. I don't think we're taking away the government's ability to do searches under proper circumstances.

JUSTICE SCALIA: Well, why isn't this a proper circumstance?

MR. DAMMEIER: The initial circumstance might be proper, but how they effectuated it was not. It was excessively intrusive. They did not -- the purpose was to find out if they were paying for enough work-related messages. They did not need to look at these, what they knew were going to be private messages. They knew -- the lieutenant had this arrangement that they could use this for personal purposes. They knew what they were going to be looking at.

JUSTICE SCALIA: They didn't know which ones were private messages, did they?

MR. DAMMEIER: Not until they read them.

JUSTICE SCALIA: Not until they read them.

MR. DAMMEIER: But there certainly -- they certainly knew what might be coming because of the arrangement that Lieutenant Duke had in place.

Here -- here I think that's --

JUSTICE ALITO: What was the arrangement that Lieutenant Duke had in place? I thought all he said was: I don't have an intent to read these,

because it's too much trouble, so if you go over and you pay me the extra, I'm not going to read them.

MR. DAMMEIER: His --

JUSTICE ALITO: Did he ever say that -- that I'm not -- that you have a privacy right in these things?

MR. DAMMEIER: No, but according -- according to Sergeant Quon's testimony, he told him: As long as you pay the overages, we're not going to read them. And that --

JUSTICE GINSBURG: Did he say "we"? He -- even Quon didn't say that. Duke said he wouldn't do it. But earlier, the -- at the meeting, the statement was made that these are open to audit. Didn't say only by Lieutenant Duke.

MR. DAMMEIER: True. True. I agree. But it was Lieutenant Duke, the one that was making the announcement that now these pagers are going to fall under the computer policy, the same lieutenant who then gave the assurance that as long as you pay the overages, we're not -- we're not going to look at them.

I mean, when you're talking about the operational reality of O'Connor, that was the operational reality. The SWAT members knew: As long as I pay the overages, my messages aren't going to be reviewed.

CHIEF JUSTICE ROBERTS: What happens, just out of curiosity, if you're -- he is on the pager and sending a message and they're trying to reach him for, you know, a SWAT team crisis? Does he -- does the one kind of trump the other, or do they get a busy signal?

MR. DAMMEIER: I don't think that's in the record. However, my understanding is that you would get it in between messages. So messages are going out and coming in at the same time, pretty much.

CHIEF JUSTICE ROBERTS: And would you know where the message was coming from?

MR. DAMMEIER: I believe so. It identifies where it's coming from. It identifies the number of where it's coming from. If you know the number, you know where it's coming from.

JUSTICE KENNEDY: And he's talking with a girlfriend, and he has a voice mail saying that your call is very important to us; we'll get back to you?

(Laughter.)

MR. DAMMEIER: Well, I think with the text messages -- and that's what we are talking about the transcripts of, were the text messages that were data transferred from device to device, and here, you know, we come back to -- I did want to touch a little bit on the Stored Communications Act having play on somebody's

1 expectation of privacy -- you know, it's -- lawfully,
2 those messages were protected. And I think, looking at
3 people's expectation of privacy, that should be a
4 component. It certainly may be not the end-all to the
5 question, but it should be a factor in determining
6 whether or not there’s going to be an expectation of
7 privacy.
8 JUSTICE SCALIA: Did -- did he know about
9 that statute? I didn't know about it.
10 MR. DAMMEIER: That's not in -- that's not
11 in the record. That is not in the record. But --
12 JUSTICE SCALIA: Can we assume he didn't?
13 MR. DAMMEIER: Right. Well, we can assume
14 that, but we also --
15 JUSTICE SCALIA: And what difference would that
16 make?
17 MR. DAMMEIER: I still don't think anything,
18 given the operational realities --
19 JUSTICE SCALIA: I don’t see how it can affect
20 his expectation of privacy, if he didn't even know about it.
21 MR. DAMMEIER: Well, it's -- it's just like
22 the California Public Records Act. We should also
23 assume he didn't know about that as well, because the --
24 Petitioners make an argument that because there is this
25 California Public Records Act, that that may diminish

one's expectation of privacy. Certainly, if we're going to have that, then we should also be having the Stored Communications Act that might enhance the --

JUSTICE SCALIA: Ignorance of the law is no excuse, is what you're saying?

JUSTICE SOTOMAYOR: Do you have any theory, or do you make any argument that Florio, Trujillo, and Quon's wife can succeed in their Fourth Amendment claims, if Quon can't?

MR. DAMMEIER: I do. We, in our brief, try to analogize that to the mail. I think when they sent messages to -- to Sergeant Quon, that was a letter that I sent. And here, the department didn't go get that letter from Sergeant Quon after -- after delivery, meaning go get it from his pager. They went to the equivalent of the Post Office, which was Arch Wireless, and got a copy off of their server. So I -- I think -- and, again, analogizing to the mail, they have an expectation of privacy while that message is in the course of delivery.

CHIEF JUSTICE ROBERTS: Well --

JUSTICE ALITO: Well, suppose it was perfectly clear that -- I mean, suppose that the department gave Mr. Quon a policy -- a statement that says: Sign this, you acknowledge that your pager is to be used only

for work and that you have no privacy interest in it whatsoever; we're going to monitor this every day. And then these other individuals sent him messages. You would still say they have an expectation of privacy in those messages?

MR. DAMMEIER: Until the point that it's on Quon's pager. I think under that scenario, that they could have obtained the messages from Quon, but they went over to Arch, the equivalent of the Post Office, and got them from them.

It's like if I -- I make a copy of a letter before I send it to somebody. You know, down the road, I might not know what happens and I might lose my expectation of privacy down the road, but that copy I kept, I think there is still an expectation.

JUSTICE SCALIA: Well, what -- when you send a text message to somebody else, aren't you quite aware that that text message will remain confidential only to the extent that either the recipient keeps it confidential -- and he can disclose it -- or somebody else who has power over the recipient or over the recipient's phone chooses to look at it? Don't -- isn't that understood when you send somebody a text message?

MR. DAMMEIER: I -- I agree with that, and --

JUSTICE SCALIA: Well, so she should have

1 understood that, you know, whoever could get ahold of
2 his phone lawfully can read the message. In other
3 words, I don't see that she's in a -- in a different
4 position from Quon himself.
5 MR. DAMMEIER: I think it's just a slightly
6 different one. I mean, first of all, they didn't
7 lawfully get it; there was a violation of the Stored
8 Communications Act to get it.
9 JUSTICE SCALIA: Well, that's a different
10 issue.
11 MR. DAMMEIER: But here, again, had they
12 gotten consent from -- from Quon and got it from him
13 directly, that's a -- that's a different story.
14 CHIEF JUSTICE ROBERTS: Well, again, it depends
15 upon their reasonable expectation. Do any of these
16 other people know about Arch Wireless? Don't they just
17 assume that once they send something to Quon, it's going
18 to Quon?
19 MR. DAMMEIER: That's -- that is true. I
20 mean, they expect --
21 CHIEF JUSTICE ROBERTS: Well, then they
22 can't have a reasonable expectation of privacy based on
23 the fact that their communication is routed through a
24 communications company.
25 MR. DAMMEIER: Well, they -- they expect

that some company, I'm sure, is going to have to be processing the delivery of this message. And --

CHIEF JUSTICE ROBERTS: Well, I didn't -- I wouldn't think that. I thought, you know, you push a button; it goes right to the other thing.

(Laughter.)

MR. DAMMEIER: Well --

JUSTICE SCALIA: You mean it doesn't go right to the other thing?

(Laughter.)

MR. DAMMEIER: It's -- I mean, it's like with e-mails. When we send an e-mail, that goes through some e-mail provider, whether it be AOL or Yahoo. It's going through some service provider. Just like when we send a letter or package, it's going through -- some provider is going to move that for us, until it gets to the end recipient. And like the mail, that message enjoys an expectation of privacy while it's with the Post Office --

JUSTICE SCALIA: Can you print these things out? Could Quon print these -- these spicy conversations out and circulate them among his buddies?

MR. DAMMEIER: Well, he could have ultimately, sure.

JUSTICE SCALIA: Well --

MR. DAMMEIER: And -- and like, when I get a piece of mail from somebody, I could do that as well, but that doesn't mean that the government gets to go to the Post Office and get my mail before I get it. I think -- I think that, you know, certainly adds a little bit to the correspondence that dealt with --

CHIEF JUSTICE ROBERTS: But just -- just to be clear: You think if these messages went straight to Quon that there'd be no problem from the point of view of the senders? I mean, no problem in searching -- getting them from Quon?

MR. DAMMEIER: I think it's certainly a harder argument for me to make --

CHIEF JUSTICE ROBERTS: Yes.

MR. DAMMEIER: -- that they have an expectation after -- after Quon has it.

CHIEF JUSTICE ROBERTS: So we have to assume for your argument to succeed that they know that this goes somewhere else and then it's processed and then it goes to Quon.

MR. DAMMEIER: Yes, but I think in today's -- I think in today's society that's -- that's a reasonable assumption to make. One --

JUSTICE SCALIA: Yes, I didn't know.

MR. DAMMEIER: I think it might have been

Florio testified that she actually called her carrier to find out, you know, if -- if the messages that she would transmit would be maintained and that was -- that they didn't maintain a copy. So there was some understanding of how the process worked.

JUSTICE ALITO: Can an officer who has one of these pagers delete messages from the pager --

MR. DAMMEIER: Yes.

JUSTICE ALITO: -- so that they can't be recovered by the department if the pager is turned into the department?

MR. DAMMEIER: Sure. Yes.

JUSTICE ALITO: They can delete them?

MR. DAMMEIER: They can delete them. Just like if they received a letter, they could be put in the shredder.

JUSTICE SCALIA: Suppose I sent somebody a letter and -- and I have privacy in that letter, and let's assume it’s intercepted at the Post Office, but I have also published the letter in a letter to the editor of the newspaper. I have written the following letter to Sergeant Quon. Do I still have a right -- a right of privacy in that letter?

MR. DAMMEIER: Well, I think then certainly your expectation may be diminished.

JUSTICE SCALIA: Well, but that's the situation here. The -- the central location that stores the message is one thing, but she's made -- made the message public effectively by sending it to Quon. Once it gets to Quon, she knows that Quon can make it public or that the employer can -- can find out about it.

MR. DAMMEIER: But that would create a free-for-all in service providers. If -- if while this message, after it’s sent and it’s in transit --

JUSTICE SCALIA: Right.

MR. DAMMEIER: It's a free-for-all. The government could just go in and --

JUSTICE SCALIA: Exactly. That -- and that's why you have the statute, because the Fourth Amendment wouldn't solve the problem, because you are effectively making it public by sending it to somebody whom you don't know is immune from disclosure. So, in order to stop the intermediary from making it public, you needed the statute. Otherwise you wouldn't need it; the Fourth Amendment would solve the problem, right?

MR. DAMMEIER: Well, certainly, obviously the statute could come into play in addition to the Fourth Amendment. But here, you know, I come back to the mail analogy. Just because at the end of the line somebody might disseminate my letter doesn't lose an

1 expectation in the copy that I make that I may keep or
2 that in the course of delivery the Post Office might
3 keep. I still enjoy an expectation -- and the Fourth
4 Amendment certainly protects that copy, that either I
5 kept or the Post Office is keeping in the course of
6 delivery.
7 Certainly, at the end of the line, that letter
8 could be published to the world, but that's not the same
9 thing as the government coming in and getting a copy of
10 it while it was being delivered.
11 JUSTICE ALITO: Are you sure that -- are you
12 sure about your answer to the question of deletion?
13 It's not like deleting something from a computer which
14 doesn't really delete it from the computer?
15 MR. DAMMEIER: Honestly, I'm not -- that's
16 not in the record, and the -- how that pager works as
17 far as deleting, I couldn't be certain that it would be
18 deleted forever. I would certainly not.
19 One -- one of the points to -- to raise,
20 too, was that most of these texts took place off duty
21 when dealing with Sergeant Quon. So, again, back to
22 looking at the actual practice that O'Connor has us look
23 at, you know, here again --
24 JUSTICE SOTOMAYOR: I thought the factual
25 record was the opposite, that in fact most of the calls

were -- not most, but a huge number of calls were happening on duty.

MR. DAMMEIER: There were -- there were a large number on-duty. I think it was broken down to where the average was 27 in a work shift and the most on one day was 80. But also they talked about -- they took about 15 seconds. So you're talking about an average of about 7 minutes during -- during a work day.

But the testimony of Sergeant Quon was that most of these were actually off-duty. And, you know, I certainly -- I think that should come into play, given the department -- they gave them pagers. And it wasn't a one-way use; it wasn't, hey, this is, you know, for the benefit of the employee. The department received a benefit. I mean, they wanted to be able to have these SWAT guys show up quickly, respond quickly, and there was a mix on -- on the reasons for these pagers.

The exchange was, we're going to let you use these for personal purposes, and given that reality, you should be able to have some -- some expectation of privacy in that use. It's like if I pick up a phone and I'm a public employee and I call my wife, I should be able to have some expectation of privacy in a conversation, especially given, you know -- you talk about guys that are on 24/7. Do they have no private

life, now? Do they not have --

JUSTICE GINSBURG: I thought the policy was limited personal use.

MR. DAMMEIER: The computer policy was limited personal use. Again, depending on how that comes into play with what Lieutenant Duke --

JUSTICE GINSBURG: But the -- the notice was we're going to treat these just like e-mails, and e-mails were limited personal use.

MR. DAMMEIER: Correct. With -- with the additional modification by -- by Duke, that you could also use them for personal purposes, from day one when the pagers were issued.

CHIEF JUSTICE ROBERTS: Thank you, counsel.

MR. DAMMEIER: Thank you.

CHIEF JUSTICE ROBERTS: Mr. Richland, you have 3 minutes remaining.

REBUTTAL ARGUMENT OF KENT L. RICHARDS

ON BEHALF OF THE PETITIONERS

MR. RICHLAND: Thank you. I would first like to just make it clear that what it is being claimed was the guarantee of privacy by Lieutenant Duke is really absolutely not that at all. And I would refer the Court to Joint Appendix page 40, which does summarize that, and it says -- here is what precisely what

1 Lieutenant Duke said: "Because of the overage
2 Lieutenant Duke went to Sergeant Quon and told him the
3 city-issued two-way pagers were considered e-mail and
4 could be audited." So that's what he said first.
5 Then he said -- he told Sergeant Quon it was
6 not his -- his intent to audit employees' text messages
7 to see if the overages were due to work-related
8 transmissions.
9 He advised Sergeant Quon he, Sergeant Quon,
10 could reimburse the city for the overages so he, Duke,
11 would not have to audit the transmission and see how
12 many messages were non-work-related. Lieutenant Duke
13 told Sergeant Quon he is doing this because if anybody
14 wished to challenge their overage, he could audit the
15 text transmissions to verify how many were
16 non-work-related, and then, finally, Lieutenant Duke
17 added, the text messages were considered public records
18 and could be audited at any time.
19 That is what is being characterized as a
20 guarantee of privacy. It's hard to see how that in any
21 way undercuts the official written policy.
22 JUSTICE SCALIA: Mr. Richland, do you take
23 any position on whether Jerilyn Quon, April Florio, and
24 Steve Trujillo stand in the same position as Sergeant
25 Quon insofar as this lawsuit is concerned?

MR. RICHLAND: We do, with respect -- in at least one respect, and that is: If Sergeant Quon loses, then we think the other plaintiffs must also lose.

JUSTICE SCALIA: Why?

MR. RICHLAND: Yes. The reason for that is that this Court has held on many occasions that, once one has sent a communication or an object to another person, they lose their expectation of privacy in --

JUSTICE SOTOMAYOR: That means the government can set up an interception mechanism on telephone transmissions, on e-mail, computer transmissions --

MR. RICHLAND: It -- it does not mean that, Justice Sotomayor.

JUSTICE SOTOMAYOR: If it doesn't mean that, answer his argument that, yes, you could take anything from Quon, but the storage -- you went to the storage facility, which is a Post Office.

MR. RICHLAND: And he says it's a Post Office, but the truth is that all of these plaintiffs admitted that they knew that this was a department-issued pager, and this wasn't a Post Office. Arch Wireless was the department's agent.

These text messages were being sent to someplace. Both the written policy and the oral policy

indicated that they were being stored ---

JUSTICE SOTOMAYOR: So you have to get into who owned --

MR. RICHLAND: Excuse me.

JUSTICE SOTOMAYOR: Whether this was a -- we have to get into the Storage Act and figure out whether this was an RCN or ACS?

MR. RICHLAND: Well, I think that -- I don't know that it's necessary to do that, because I think that all that must be determined is -- and I don't think whether it's an ECS or RCS is -- you would require that to determine who owned it, because it was clear that Arch acted solely as the city's agent.

JUSTICE SCALIA: Whoa, whoa. I'm not sure you’re doing the city a favor by making Arch the city's agent --

MR. RICHLAND: I understand --

JUSTICE SCALIA: -- as opposed to an independent contractor who is doing business with the city.

MR. RICHLAND: The point is --

JUSTICE SCALIA: You sure you want to live with that?

MR. RICHLAND: I don't mean "agent" in -- in the most literal sense, Justice Scalia.

JUSTICE SCALIA: Oh, okay.

MR. RICHLAND: What I mean is that they were -- in effect, when there was a delivery to Arch Wireless, it was a delivery to the city. And all of these individuals knew that this was city equipment, and, therefore, this was being delivered to the city.

CHIEF JUSTICE ROBERTS: Thank you, counsel.

The case is submitted.

(Whereupon, at 12:08 p.m., the case in the above-entitled matter was submitted.)

In The

Supreme Court of the United States

CITY OF ONTARIO, ONTARIO POLICE DEPARTMENT, and LLOYD SCHARF,

Petitioners,

v.

JEFF QUON, JERILYN QUON, APRIL FLORIO, and STEVE TRUJILLO,

Respondents.

On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

PETITION FOR A WRIT OF CERTIORARI

DIMITRIOS C. RINOS
Rinos & Martin, LLP
17862 East 17th Street, Suite 104
Tustin, California 92780
(714) 734-0400

KENT L. RICHLAND
(Counsel of Record)
KENT J. BULLARD
Greines, Martin, Stein & Richland LLP
5900 Wilshire Boulevard, 12th Floor
Los Angeles, California 90036
(310) 859-7811

Counsel for Petitioners

COCKLE LAW BRIEF PRINTING CO. (800) 225-6964
OR CALL COLLECT (402) 342-2831

Blank Page

QUESTIONS PRESENTED

While individuals do not lose Fourth Amendment rights merely because they work for the government, some expectations of privacy held by government employees may be unreasonable due to the "operational realities of the workplace." *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (plurality). Even if there exists a reasonable expectation of privacy, a warrantless search by a government employer – for non-investigatory work-related purposes or for investigations of work-related misconduct – is permissible if reasonable under the circumstances. *Id.* at 725-26 (plurality). The questions presented are:

1. Whether a SWAT team member has a reasonable expectation of privacy in text messages transmitted on his SWAT pager, where the police department has an official no-privacy policy but a non-policymaking lieutenant announced an informal policy of allowing some personal use of the pagers.

2. Whether the Ninth Circuit contravened this Court's Fourth Amendment precedents and created a circuit conflict by analyzing whether the police department could have used "less intrusive methods" of reviewing text messages transmitted by a SWAT team member on his SWAT pager.

3. Whether individuals who send text messages to a SWAT team member's SWAT pager have a reasonable expectation that their messages will be free from review by the recipient's government employer.

PARTIES TO THE PROCEEDING

Petitioners (defendants and appellees below):

CITY OF ONTARIO, ONTARIO POLICE DEPARTMENT, and LLOYD SCHARF

Respondents (plaintiffs and appellants below):

JEFF QUON, JERILYN QUON, APRIL FLORIO, and STEVE TRUJILLO

Additional defendants and appellees below:

DEBBIE GLENN

ARCH WIRELESS OPERATING COMPANY, INCORPORATED

Additional plaintiff below:

DOREEN KLEIN

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF CONTENTS – Continued

Page

APPENDIX

TABLE OF AUTHORITIES

Page

FEDERAL CASES

TABLE OF AUTHORITIES – Continued

Page

TABLE OF AUTHORITIES – Continued

Page

STATE CASES

CONSTITUTION AND FEDERAL STATUTES

STATE STATUTES

MISCELLANEOUS

TABLE OF AUTHORITIES – Continued

Page

Blank Page

Petitioners City of Ontario, Ontario Police Department, and Lloyd Scharf (collectively, Ontario defendants) respectfully petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit.

OPINIONS BELOW

The Ninth Circuit's opinion is reported at 529 F.3d 892 (9th Cir. 2008). App., *infra*, 1-40. Its order denying rehearing and rehearing en banc, including a one-judge concurring opinion and a seven-judge dissenting opinion, is reported at 554 F.3d 769 (9th Cir. 2009). App., *infra*, 124-150. The opinion of the United States District Court for the Central District of California is reported at 445 F. Supp. 2d 1116 (C.D. Cal. 2006). App., *infra*, 41-116.

JURISDICTION

The Ninth Circuit issued its decision on June 18, 2008. App., *infra*, 1. Petitioners timely filed a petition for rehearing and rehearing en banc, which was denied on January 27, 2009, with one judge concurring in and seven judges dissenting from the denial of rehearing en banc. App., *infra*, 124-125, 136. This Court has jurisdiction under 28 U.S.C. section 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the placed to be searched, and the persons or things to be seized. U.S. Const. amend. IV.

Section 1983 of Title 42 of the United States Code provides:

> Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress, except that in any action brought against a judicial officer for an act or omission taken in such officer's judicial capacity, injunctive relief shall not be granted unless a declaratory decree was violated or declaratory relief was unavailable. For the purposes of this section, any Act of Congress applicable exclusively to

the District of Columbia shall be considered to be a statute of the District of Columbia. 42 U.S.C. § 1983.

STATEMENT OF THE CASE

1. Ontario Police Department SWAT team Sergeant Jeff Quon used his Department-issued text-messaging pager to exchange hundreds of personal messages – many sexually explicit – with, among others, his wife (Jerilyn Quon), his girlfriend (April Florio), and a fellow SWAT team sergeant (Steve Trujillo). He did so notwithstanding the City of Ontario's written "Computer Usage, Internet and E-mail Policy" – which both Sergeants Quon and Trujillo acknowledged in writing – that permitted employees only limited personal use of City-owned computers and associated equipment, including e-mail systems, and warned them not to expect privacy in such use. App., *infra*, 151-157.

The City's written policy advised employees, among other things, that:

- "The use of these tools for personal benefit is a significant violation of City of Ontario Policy." App., *infra*, 152.
- "The use of any City-owned computer equipment, . . . e-mail services or other City computer related services for personal benefit or entertainment is

> prohibited, with the exception of 'light personal communications.'" *Id.*

The policy explained that "[s]ome incidental and occasional personal use of the e-mail system is permitted if limited to 'light' personal communications[,]" which "may consist of personal greetings or personal meeting arrangements." App., *infra*, 153.

As for privacy and confidentiality, the policy informed employees they should expect none:

- "The City of Ontario reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." App., *infra*, 152.
- "Access to the Internet and the e-mail system is not confidential;. . . . As such, these systems should not be used for personal or confidential communications. Deletion of e-mail or other electronic information may not fully delete the information from the system." App., *infra*, 153.
- "[E-mail] messages are also subject to 'access and disclosure' in the legal system and the media." *Id.*

The policy additionally stated that "[t]he use of inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language in the e-mail

system will not be tolerated." *Id.* When the Department obtained text-messaging pagers to facilitate logistical communications among SWAT team officers, it informed the officers that the e-mail policy applied to pager messages. App., *infra*, 5, 29, 48.

Under the City's contract with its wireless provider – Arch Wireless Operating Company, Inc. – each pager had a monthly character limit, above which the City had to pay extra. App., *infra*, 6, 45. The officer in charge of administration of the pagers – Lieutenant Steve Duke – had an informal arrangement whereby he would not audit pagers that had exceeded the monthly character limit if the officers agreed to pay for any overages. App., *infra*, 6-8, 29-30. Certain officers, including Sergeant Quon, repeatedly exceeded the character limit. *See* App., *infra*, 8, 50-51. In response to Lieutenant Duke's report that he was tired of being a bill collector, the Chief of Police ordered a review of the pager transcripts for the two officers with the highest overages – one of whom was Sergeant Quon – to determine whether the City's monthly character limit was insufficient to cover business-related messages. App., *infra*, 8, 51. The Department then obtained the pager transcripts for the two officers from Arch Wireless. App., *infra*, 8-9.

After initial Department review, the matter was referred to internal affairs to determine whether Sergeant Quon was wasting time attending to personal issues while on duty. App., *infra*, 9. Sergeant

Patrick McMahon, of internal affairs, with the help of Sergeant Debbie Glenn, redacted the transcripts to eliminate messages that did not occur on duty. App., *infra*, 9, 56; *see also* Supplemental Excerpts of Record ("SER") 251. During the month under review, Sergeant Quon sent and received 456 personal messages while on duty – on average per shift, 28 messages, only 3 of which were business related. SER 254; *see also* App., *infra*, 54-55. "Some of these messages were directed to or from his wife, [plaintiff] Jerilyn Quon," who was a former Department employee, "while others were directed to and from his mistress, [plaintiff April] Florio," who was a police dispatcher. App., *infra*, 54-55; *see also* SER 303, 307. Many of their text messages were not "light personal communications," as defined in the policy, but rather were, in the district court's words, "to say the least, sexually explicit in nature." App., *infra*, 54; *see also* SER 532, 539, 546.

2. Sergeant Quon and his text-messaging partners sued the Chief of Police, the City, the Department, and others, alleging Fourth Amendment violations under 42 U.S.C. section 1983. *See* App., *infra*, 58.[1] On cross-motions for summary judgment, the district court first held that Sergeant Quon had a reasonable expectation of privacy in his pager

[1] Plaintiffs made other claims and sued other defendants, including a separately represented police sergeant – Debbie Glenn – and Arch Wireless. *See* App., *infra*, 58. For brevity's sake, we do not discuss those claims.

transcripts as a matter of law under the "operational realities of the workplace" standard from *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (plurality). App., *infra*, 88-97. The court based its decision on Lieutenant Duke's informal policy that "he would *not* audit their pagers so long as they agreed to pay for any overages." App., *infra*, 90 (emphasis in original).

The court next considered whether reviewing the transcripts was reasonable under the circumstances. App., *infra*, 97. It determined there was a genuine issue of material fact as to "the actual *purpose* or *objective* Chief Scharf sought to achieve." *Id.* (emphasis in original). The court reasoned that the transcript review was *not* reasonable if it "was meant to ferret out misconduct by determining whether the officers were 'playing games' with their pagers or otherwise 'wasting a lot of City time conversing with someone about non-related work issues.'" App., *infra*, 98. But the court reasoned the transcript review *was* reasonable if the purpose was to "determin[e] the utility or efficacy of the existing monthly character limits." App., *infra*, 99. The court also determined that the scope of the audit was reasonable for the purpose of determining the efficacy of the character limit. App., *infra*, 103.

Denying summary judgment, the district court ruled that a jury would decide "which was the primary purpose of the audit." *Id.* The court also rejected Chief Scharf's qualified immunity defense, reasoning that if the jury found that he "order[ed] the audit, under the guise of seeking to ferret out

misconduct," he would not be entitled to qualified immunity. App., *infra*, 104, 108.

A jury found that Chief Scharf's purpose in ordering review of the transcripts was to determine the character limit's efficacy. App., *infra*, 119. As a result, the district court ruled that there was no Fourth Amendment violation, and judgment was entered in favor of defendants. App., *infra*, 119-120.

3. Plaintiffs appealed. On appeal, Ontario defendants argued that they should have been granted summary judgment in their favor because, as a matter of law, plaintiffs had no reasonable expectation of privacy and the search was reasonable under either purpose submitted to the jury.

The Ninth Circuit reversed, in an opinion authored by Judge Wardlaw and joined by Judge Pregerson and District Judge Leighton (sitting by designation). The panel ruled that plaintiffs were entitled to summary judgment in their favor against the City and the Department. App., *infra*, 40. Applying the *O'Connor* plurality's "operational realities of the workplace" standard, 480 U.S. at 717, the panel concluded Sergeant Quon had a reasonable expectation of privacy because of Lieutenant Duke's informal policy of allowing officers to pay for overages. App., *infra*, 29.

The panel also held that the other three plaintiffs had a reasonable expectation of privacy in messages they had sent to Sergeant Quon's pager, but not based on Lieutenant Duke's bill-paying arrangement. App.,

infra, 27 n.6. Rather, analogizing text messages to e-mail messages, regular mail, and telephone communications, App., *infra*, 23-28, it concluded that, "[a]s a matter of law, Trujillo, Florio, and Jerilyn Quon had a reasonable expectation that the Department would not review their messages absent consent from either a sender or recipient of the text messages." App., *infra*, 28-29.

In evaluating the reasonableness of the search under the *O'Connor* framework, the panel concluded that given the jury's special verdict that the purpose of the search was administrative – to determine the character limit's efficacy – the search was reasonable at its inception to ensure that officers were not being required to pay for work-related expenses. App., *infra*, 33-34. Nevertheless, relying on *Schowengerdt v. General Dynamics Corp.*, 823 F.2d 1328, 1336 (9th Cir. 1987), the panel reasoned that if "less intrusive methods" were feasible, then the search was unreasonable. App., *infra*, 35. The panel hypothesized that there were "a host of simple ways" the Department could have conducted its administrative investigation without intruding on plaintiffs' Fourth Amendment rights. *Id.* The panel therefore concluded that the search violated the Fourth Amendment as a matter of law. App., *infra*, 36, 39.

The panel determined, however, that Chief Scharf was entitled to qualified immunity because "there was no clearly established law regarding whether users of text-messages that are archived, however temporarily, by the service provider have a

reasonable expectation of privacy in those messages." App., *infra*, 37-38.

4. The City and the Department petitioned for panel rehearing and rehearing en banc on the grounds that: (1) the panel's ruling on a government employee's reasonable expectation of privacy in text messaging on a government-issued pager dramatically undermined the "operational realities of the workplace" standard of *O'Connor*, 480 U.S. at 717 (plurality); (2) the panel erroneously extended Fourth Amendment protection with its sweeping ruling that individuals who send text messages to a government employee's workplace pager – rather than to a privately owned pager – reasonably expect that their messages will be free from the employer's review; and (3) the panel's reliance on *Schowengerdt*'s "less intrusive methods" analysis required review to secure uniformity of the court's decisions in light of this Court's and other circuits' authorities "repeatedly" rejecting the "existence of alternative 'less intrusive' means" as a basis for evaluating the reasonableness of government activity under the Fourth Amendment, as exemplified in *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 629 n.9 (1989) (citations omitted) (collecting cases).

The United States filed an amicus curiae brief supporting the petition. App., *infra*, 158-180. CSAC Excess Insurance Authority – a California Joint Powers Authority representing 54 of California's 58 counties – sought leave to file an amicus curiae brief supporting the petition.

Panel rehearing and rehearing en banc were denied. App., *infra*, 125. However, Judge Ikuta, joined by six other judges, dissented from the denial of rehearing en banc. App., *infra*, 136-150. The dissent disagreed with the panel's conclusion that the search violated the Fourth Amendment for two main reasons:

- "First, in ruling that the SWAT team members had a reasonable expectation of privacy in the messages sent from and received on pagers provided to officers for use during SWAT emergencies, the panel undermines the standard established by the Supreme Court in *O'Connor v. Ortega*, 480 U.S. 709 (1987), to evaluate the legitimacy of non-investigatory searches in the workplace." App., *infra*, 136-137.
- "Second, the method used by the panel to determine whether the search was reasonable conflicts with binding Supreme Court precedent, in which the Court has repeatedly held that the Fourth Amendment does not require the government to use the 'least intrusive means' when conducting a 'special needs' search. *See Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie County v. Earls*, 536 U.S. 822, 837 (2002); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995); *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602,

629 n.9 (1989)." App., *infra*, 137 (parallel citations omitted).

Judge Wardlaw filed an opinion concurring in the denial of rehearing en banc, arguing that the dissent was mistaken as to the facts and the law. App., *infra*, 125-136. No other judges joined the concurrence.

REASONS TO GRANT THE PETITION

The Ninth Circuit panel viewed "[t]he recently minted standard of electronic communication via e-mails, text messages, and other means" as "open[ing] a new frontier in Fourth Amendment jurisprudence that has been little explored." App., *infra*, 23-24. The panel's opinion literally "wowed" privacy advocates,[2] and it surprised more mainstream media.[3] For good

[2] *E.g.*, Jennifer Granick, *New Ninth Circuit Case Protects Text Message Privacy from Police and Employers*, Electronic Frontier Foundation, June 18, 2008, http://www.eff.org/deeplinks/2008/06/new-ninth-circuit-case-protects-text-message-priva ("[E]ven if your employer pays for your use of third party text or email services, your boss can't get copies of your messages from that provider without your permission. Wow.").

[3] *E.g.*, Jennifer Ordoñez, *They Can't Hide Their Pryin' Eyes – An Appeals Court Ruling Makes It More Difficult For Employers To Sniff Around In Workers' Electronic Communications*, Newsweek, July 14, 2008, at 22 ("For desk jockeys everywhere, it has become as routine as a tour of the office-supply closet: the consent form attesting that you understand and accept that any e-mails you write, Internet sites you visit or business you conduct on your employer's computer network are subject to inspection.").

reason: public and private employers alike typically have in place policies establishing that employees should have no expectation of privacy in electronic communications and other computer usage on employer-owned equipment. As the United States explained in its amicus brief in the Ninth Circuit, these policies are intended to "prevent abuse and promote the public's safety and security." App., *infra*, 162-163.

The opinion dissenting from the denial of rehearing en banc summarized that

> [b]y holding that a SWAT team member has a reasonable expectation of privacy in the messages sent to and from his SWAT pager, despite an employer's express warnings to the contrary and "operational realities of the workplace" that suggest otherwise, and by requiring a government employer to demonstrate that there are no . . . less intrusive means available to determine whether its wireless contract was sufficient to meet its needs, the panel's decision is contrary to "the dictates of reason and common sense" as well as the dictates of the Supreme Court.

App., *infra*, 149-150.

The dissenting judges were right. To warrant Fourth Amendment protection, a government employee's expectation of privacy must be one "'that society is prepared to consider reasonable'" under the "operational realities of the workplace." *O'Connor v.*

Ortega, 480 U.S. 709, 715, 717 (1987) (plurality) (citation omitted). Concluding that a government employee has a reasonable expectation of privacy in text messages sent and received on a pager issued by his employer, the Ninth Circuit panel mistakenly reasons that the employer's explicit no-privacy policy is abrogated by a lower-level supervisor's informal arrangement allowing some personal use of the pager, and discounts entirely the potential disclosure of the messages under public records laws. As the dissent notes: "In doing so, the panel improperly hobbles government employers from managing their workforces." App., *infra*, 137.

And in holding that the scope of the government employer's administrative review of transcripts of the employee's text messages was unreasonable, the Ninth Circuit relied on a "less intrusive methods" analysis that this Court and multiple other circuits have repeatedly rejected as a basis for evaluating the reasonableness of government activity under the Fourth Amendment. *E.g.*, *Skinner*, 489 U.S. at 629 n.9 (citations omitted). The panel's "less intrusive methods" approach not only conflicts with this Court's and other circuits' authority, but also, as the dissent discerns, "makes it exceptionally difficult for public employers to go about the business of running government offices." App., *infra*, 137.

Making matters worse, the Ninth Circuit extends Fourth Amendment protection beyond any reasonable parameters by concluding that even individuals who knowingly send text messages *to* a government

employee's *workplace* pager – rather than to a privately owned pager – reasonably expect that their messages will be free from the recipient's employer's review. App., *infra*, 28. The panel thus further hobbles employers' ability to monitor electronic communications and enforce no-confidentiality policies.

Below we demonstrate that certiorari should be granted (a) to restore reasonableness to the *O'Connor* "operational realities of the workplace standard" as it applies to expectations of privacy in electronic communications in the workplace; (b) to settle once and for all the split among the circuits on the applicability of a "less-intrusive means" analysis under the Fourth Amendment; and (c) to curb the Ninth Circuit's startling extension of Fourth Amendment privacy rights to individuals who send electronic communications to government employees' government-issued communications devices.

Simply put, the SWAT team sergeant failed to comport himself as a reasonable officer would have, and he and the other plaintiffs embarrassed themselves through their lack of restraint in using a City-owned pager for personal and highly private communications. The City of Ontario should not have to pay for that in this case, nor should other government employers be hobbled by the Ninth Circuit's ruling. Certiorari should be granted.

I. THE NINTH CIRCUIT OPINION UNDERMINES THE "OPERATIONAL REALITIES OF THE WORKPLACE" STANDARD FOR MEASURING FOURTH AMENDMENT PROTECTION IN GOVERNMENT WORKPLACES BY ERRONEOUSLY HOLDING THAT A POLICE LIEUTENANT'S INFORMAL POLICY CREATES A REASONABLE EXPECTATION OF PRIVACY IN TEXT MESSAGING ON A POLICE DEPARTMENT PAGER IN THE FACE OF THE DEPARTMENT'S EXPLICIT NO-PRIVACY POLICY AND POTENTIAL DISCLOSURE OF THE MESSAGES AS PUBLIC RECORDS.

The Department had a written no-privacy policy for e-mail and computer use, Sergeant Quon signed an acknowledgment of it, and he attended a meeting at which it was made clear that the policy fully applied to the pagers. App., *infra*, 29, 156; *see also* SER 320, 463-64.) "If that were all," the Ninth Circuit panel reasoned, the case would be governed by the rule that employees have no reasonable expectation of privacy where they have notice of employer policies permitting searches. App., *infra*, 29 (citing *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) and *Bohach v. City of Reno*, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996)). To that point, the panel's reasoning is a straightforward application of *O'Connor*'s "operational realities of the workplace" standard, to which government employers and employees have become accustomed. *See, e.g.*, *Biby v. Bd. of Regents*,

419 F.3d 845, 850-51 (8th Cir. 2005); *United States v. Angevine*, 281 F.3d 1130, 1134-35 (10th Cir. 2002); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000).

But the panel concluded that "such was not the 'operational reality' at the Department" because "'Lieutenant Duke made it clear to the staff, and to Quon in particular, that he would *not* audit their pagers so long as they agreed to pay for any overages.'" App., *infra*, 30. Here the panel mistakenly relied on Lieutenant Duke's informal accommodation – in the face of the Department's express policy – as determinative of whether an expectation of privacy in the text messages was reasonable.

The district court aptly characterized Lieutenant Duke's bill-paying arrangement as his "generous way of streamlining administration and oversight over the use of the pagers because, as he reminded [Sergeant] Quon, he could, 'if anybody wished to challenge their overage, . . . audit the text transmissions to verify how many were non-work related.'" App., *infra*, 50. Given the official, explicit, Department-wide "no privacy" policy as to all electronic communications, an officer could not reasonably interpret Lieutenant Duke's informal policy to mean that the Department would never review messages sent on the Department's pagers without first getting the officer's additional consent.

As the panel acknowledged, but dismissed as unimportant, Lieutenant Duke was not a Department

policymaker. App., *infra*, 31. Thus, holding the City and Department liable based on Lieutenant Duke's informal policy amounts to an end-run around well-established principles that only official policies or acts of official policymakers may give rise to municipal liability under 42 U.S.C. section 1983. *City of St. Louis v. Praprotnik*, 485 U.S. 112, 127 (1988); *Monell v. Dep't of Soc. Services*, 436 U.S. 658, 694 (1978); *see also Bennett v. City of Eastpointe*, 410 F.3d 810, 819 (6th Cir. 2005) (plaintiffs could not base section 1983 claims on memorandum that had been written by current police chief when he "was simply a lieutenant, and not a policy-making official").

The thousands of government offices throughout the nation have supervisors like Lieutenant Duke attempting to oversee employees' use of a seemingly never-ending stream of new technologies, from e-mailing to text messaging to instant messaging to using Twitter. It simply isn't realistic to avoid informal statements that arguably contradict formal no-privacy policies. But that squarely raises the issue of whether it is reasonable under the Fourth Amendment for government employees to ignore official, explicit no-privacy policies to the contrary.

Within the operational realities of a police department, the answer is certainly no. "Given that the pagers were issued for use in SWAT activities, which by their nature are highly charged, highly visible situations, it is unreasonable to expect that messages sent on pagers provided for communication among SWAT team members during those

emergencies would not be subsequently reviewed by an investigating board, subjected to discovery in litigation arising from the incidents, or requested by the media." App., *infra*, 142 (Ikuta, J., dissenting from denial of rehearing en banc.). "The public expects [police] officers to behave with a high level of propriety, and, unsurprisingly, is outraged when they do not do so." *Dible v. City of Chandler*, 515 F.3d 918, 928 (9th Cir. 2008). A reasonable police officer understands these operational realities and thus cannot reasonably expect privacy in text messages on a Department-issued pager, particularly messages sent while on duty.

A related operational reality is the public's potential access to the pager transcripts under the California Public Records Act ("CPRA") (Cal. Gov't Code § 6250, *et seq.*). The panel reasoned that the CPRA would not preclude a reasonable expectation of privacy – even if the pager messages were public records – absent evidence that CPRA requests were sufficiently "'widespread or frequent.'" App., *infra*, 32. But that misses the point. As the judges dissenting from denial of rehearing en banc correctly discerned, "[g]overnment employees in California are well aware that every government record is potentially discoverable at the mere request of a member of the public, and their reasonable expectation of privacy in such public records is accordingly reduced." App., *infra*, 142-143.

Whether an expectation of privacy was objectively reasonable must be evaluated under the

totality of these operational realities, not by ignoring the City's no-privacy policy and by downplaying the potential for public disclosure. Permitting informal accommodations for some personal use to trump government employers' explicit no-privacy policies threatens to disembowel the "operational realities" standard. In its amicus curiae brief in the Ninth Circuit, the United States warned that the panel's error in relying on the informal policy of a non-policymaker "puts into doubt employee agreements and privacy policies used across the private sector and government to assist internal investigators in identifying possible corruption, threats to security, or abuse of government resources or authority." App., *infra*, 172-173.

And, with the panel's opinion extant, government employers would be wise to curtail *any* flexibility in electronic communications policies in order to maintain the viability of no-privacy policies. This Court therefore should take this opportunity to restore reasonableness and common sense to *O'Connor*'s "operational realities of the workplace" standard.

II. THE NINTH CIRCUIT OPINION CONTRAVENES THIS COURT'S DECISIONS AND CREATES A SPLIT AMONG THE CIRCUITS ON WHETHER A "LESS INTRUSIVE MEANS" ANALYSIS MAY BE APPLIED TO DETERMINE WHETHER A SEARCH IS REASONABLE UNDER THE FOURTH AMENDMENT.

This Court has "repeatedly" rejected the "existence of alternative 'less intrusive' means" as a basis for evaluating the reasonableness of government activity under the Fourth Amendment. *Skinner*, 489 U.S. at 629 n.9 (collecting cases) (citations omitted). "It is obvious that the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers . . . because judges engaged in post hoc evaluations of government conduct can almost always imagine some alternative means by which the objectives of the government might have been accomplished." *Id.* (internal citations and quotations omitted).

Until this panel opinion, the circuit courts uniformly heeded this Court's admonitions. The opinion dissenting from the denial of rehearing en banc points out – and the concurring opinion does not contest – that "[s]even other circuits have followed the Supreme Court's instruction and explicitly rejected a less intrusive means inquiry in the Fourth Amendment context." App., *infra*, 147-149 (citing *Davenport v. Causey*, 521 F.3d 544, 552 (6th Cir.

2008); *Lockhart-Bembery v. Sauro*, 498 F.3d 69, 76 (1st Cir. 2007); *Cassidy v. Chertoff*, 471 F.3d 67, 79 (2d Cir. 2006); *Shell v. United States*, 448 F.3d 951, 956 (7th Cir. 2006); *United States v. Prevo*, 435 F.3d 1343, 1348 (11th Cir. 2006); *Shade v. City of Farmington*, 309 F.3d 1054, 1061 (8th Cir. 2002); *United States v. Melendez-Garcia*, 28 F.3d 1046, 1052 (10th Cir. 1994)). The panel opinion, however, creates a split in the circuits by reintroducing a "less intrusive means" analysis into Fourth Amendment jurisprudence.

The opinion concurring in the denial of rehearing en banc argues that the panel did not actually engage in a less intrusive means analysis, but as the dissent notes, the panel opinion "does exactly" that. App., *infra*, 145.

- The panel quoted the Ninth Circuit's opinion in *Schowengerdt v. General Dynamics Corp.*, 823 F.2d 1328 (9th Cir. 1987), for the proposition that "'if less intrusive methods were feasible, . . . the search would be unreasonable.'" App., *infra*, 35 (quoting *Schowengerdt*, 823 F.2d at 1336).

- The panel posited that "[t]here were a host of simple ways to verify the efficacy of the 25,000 character limit (if that, indeed, was the intended purpose) without intruding on [plaintiffs'] Fourth Amendment rights." App., *infra*, 35.

- The panel provided examples that were never even suggested by plaintiffs. *Id.*

It is difficult to understand how this approach could *not* be considered a "less intrusive means" test.

As the dissent from the denial of rehearing cogently observed, "[r]ather than evaluate whether the search '*actually* conducted' by the police department was 'reasonably related to the objectives of the search and not excessively intrusive in light of [its purpose], as *O'Connor* requires us to do, 480 U.S. at 726, . . . (emphasis added), the panel looks at what the police department *could* have done." App., *infra*, 145 (parallel citation omitted). The panel thus engaged in precisely the kind of "post-hoc exercise of imagining some other path of conduct the government could have taken," *Taylor v. O'Grady*, 888 F.2d 1189, 1195 (7th Cir. 1989), or "'Monday morning quarterbacking[,]'" *Shade*, 309 F.3d at 1061, that other circuits have concluded is not permissible under this Court's Fourth Amendment jurisprudence.

The opinion concurring in the denial of rehearing en banc also suggests that this Court's prohibition against using a "less intrusive means" analysis applies only to "special needs" searches and states that this case did *not* involve a 'special needs' search." App., *infra*, 135 (citation omitted). The concurrence is wrong on both points.

First, even though cases in which this Court has rejected the "least restrictive means" mode of analysis "have often involved circumstances in which the

government had engaged in 'years of investigation and study' that resulted in 'reasonable conclusions' that the government conduct was necessary," App., *infra*, 135 (citing *Skinner*, 489 U.S. at 629 n.9), many such cases have *not* involved elaborate deliberative processes. *E.g.*, *United States v. Sharpe*, 470 U.S. 675, 686-87 (1985) (20-minute *Terry* stop of pickup truck driver by DEA agent); *Illinois v. Lafayette*, 462 U.S. 640, 647 (1983) (administrative search of arrestee's personal effects at police station); *Cady v. Dombrowski*, 413 U.S. 433, 447 (1973) (warrantless search of car trunk). Nor have other circuits read this Court's precedents in such a limited manner. *E.g.*, *Lockhart-Bembery*, 498 F.3d at 71, 76 (police officer giving routine police assistance to disabled motorist whose car posed a traffic hazard on a busy road and ordering motorist to move car); *Shade*, 309 F.3d at 1057, 1061 (police officer's pat-down search of student for knife); *Melendez-Garcia*, 28 F.3d at 1052 (*Terry* stop of automobile to search for drugs).

Second, this Court in *O'Connor* expressly concluded that public employer searches *are* "special needs" searches: "In sum, we conclude that the 'special needs, beyond the normal need for law enforcement make the . . . probable-cause requirement impracticable,' . . . for legitimate work-related, noninvestigatory intrusions as well as investigations of work-related misconduct are present in the context of government employment." 480 U.S. at 725 (plurality); *accord*, *id.* at 732 (Scalia, J., concurring in the judgment) ("'[S]pecial needs' are

present in the context of government employment.") As *O'Connor* explained, "public employers have a direct and overriding interest in ensuring that the work of the agency is conducted in a proper and efficient manner," and must be "given wide latitude" in carrying out administrative searches, which serve to "ensure the efficient and proper operation of the agency." 480 U.S. at 723-24 (plurality).

Far from giving the Department wide latitude, the panel expressly followed *Schowengerdt*, in which the Ninth Circuit had added a "less intrusive methods" and "no broader than necessary" gloss to the *O'Connor* analysis. 823 F.2d at 1336. But this gloss – in addition to conflicting with the opinions of the seven circuits listed above – is incompatible with *O'Connor* itself.

Further contravening *O'Connor*, the panel's suggested "less intrusive" means effectively require employees' consent (notwithstanding their agreement to the employer's no-privacy policy) for the employer to investigate at all. While valid consent may obviate a warrant or probable cause, 4 Wayne R. LaFave, *Search & Seizure* (4th ed. 2004) § 8.1, at 4-5 & n.9, probable cause is not needed for a public employer's search under *O'Connor*, 480 U.S. at 725 (plurality); *id.* at 732 (Scalia, J., concurring in the judgment).

Instead of hypothesizing "less intrusive" means, the panel should have "'balanc[ed] [the search's] intrusion on the individual's Fourth Amendment interests against its promotion of legitimate

governmental interests.'" *Vernonia*, 515 U.S. at 652-53 (citations omitted). But the panel failed to balance the interests: It didn't weigh the plaintiffs' interests in using Sergeant Quon's *Department-issued* pager for personal communications – even highly private, sexually graphic ones – while he was on duty, *see* SER 532, 539, 546, against the Department's "direct and overriding interest in ensuring that the work of the agency is conducted in a proper and efficient manner." 480 U.S. at 724 (plurality); *see also Dible*, 515 F.3d at 928 ("[T]he interest of the City in maintaining the effective and efficient operation of the police department is particularly strong.").

The panel opinion gives no recognition to *O'Connor*'s teaching that "privacy interests of government employees in their place of work . . . are far less than those found at home or in some other contexts." *O'Connor*, 480 U.S. at 725 (plurality). Just as the *O'Connor* plurality explained that "[t]he employee may avoid exposing personal belongings at work by simply leaving them at home," *id.*, the opinion dissenting from the denial of rehearing en banc in this case aptly explains that "Quon could have avoided exposure of his sexually explicit text messages simply by using his own cell phone or pager." App., *infra*, 143. The City and Department should not be punished because a legitimate workplace search happened to turn up sexually explicit messages that plaintiffs need not and should not have sent on government-issued equipment in the first place. *Cf. Simons*, 206 F.3d at 400 (government

employer "did not lose its special need for 'the efficient and proper operation of the workplace' [under *O'Connor*] merely because the evidence obtained was evidence of a crime").

In fact, as Ontario defendants argued in the Ninth Circuit, the transcript review was reasonable even if Chief Scharf's purpose in ordering it was to investigate misconduct. Under *O'Connor*, even if there exists a reasonable expectation of privacy, a warrantless search may be legal if it is both work-related – for example to investigate work-related misconduct – and reasonable under the circumstances. 480 U.S. at 724-25 (plurality); *id.* at 732 (Scalia, J., concurring in the judgment).[4]

Put simply, "the relevant question is whether th[e] intrusion upon privacy is one that a reasonable employer might engage in." *Vernonia*, 515 U.S. at 665

---

[4] The opinion concurring in the denial of rehearing en banc contends the City did not file its own appeal and "for reasons of its own, was quite content to have the jury find a legitimate purpose for Chief Scharf's search." App., *infra*, 131. However, the concurrence omits that the City argued that the Ninth Circuit should affirm on the alternative grounds that the City was entitled to *summary judgment in its favor* because, as a matter of law, plaintiffs had no reasonable expectation of privacy and the review of the pager transcripts was reasonable under *either* purpose submitted to the jury by the District Court. The City relied on the "firmly entrenched rule" that, even without cross-appealing, an appellee may assert any ground for affirmance that is apparent on the record as long as the appellee does not seek to enlarge the relief obtained below. *El Paso Natural Gas Co. v. Neztsosie*, 526 U.S. 473, 479-80 (1999).

(citing *O'Connor*). Here, the answer is yes. But the panel's decision encourages government employees to act unreasonably and prevents government employers – even ones with explicit no-privacy policies – from undertaking reasonable searches without the employees' further consent.

III. THE NINTH CIRCUIT OPINION EXTENDS FOURTH AMENDMENT PROTECTION BEYOND REASONABLE LIMITS BY HOLDING THAT INDIVIDUALS SENDING TEXT MESSAGES TO A GOVERNMENT EMPLOYEE'S GOVERNMENT-ISSUED PAGER HAVE A REASONABLE EXPECTATION OF PRIVACY.

The Ninth Circuit's sweeping holding that plaintiffs Trujillo, Florio, and Jerilyn Quon reasonably expected that their messages to Sergeant Quon would be free from Department review is mistaken and further damages government employers' ability to effectively use and monitor communications equipment.

The panel began by asserting that "[t]he extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question." App., *infra*, 23. Next the panel framed the issue as if these plaintiffs had sent text messages to Sergeant Quon on his personal pager and as if he had his own account with Arch Wireless, ignoring the fact that they had sent the messages to a police officer on his Department-issued pager. *See* App., *infra*, 24 ("Do users of text

messaging services such as those provided by Arch Wireless have a reasonable expectation of privacy in their text messages stored on the service provider's network?"). With respect to these plaintiffs, as opposed to Sergeant Quon, the panel expressly did *not* rely on Lieutenant Duke's bill-paying arrangement, App., *infra*, 27 n.6, and the opinion is silent as to their knowledge of it. In fact, the panel fails to account for the fact that the other plaintiffs were fully aware that they were sending messages to Sergeant Quon's Department-issued pager.[5]

Analogizing text messages to telephone calls, regular mail, and e-mail, the panel broadly held that plaintiffs had a reasonable expectation of privacy in the content of messages they sent to Sergeant Quon such that their consent or his consent was required for the Department to review the messages. *See* App.,

---

[5] Sergeant Trujillo was a fellow member of the SWAT team and also using a Department-issued pager himself. *See* App., *infra*, 2, 5. Police dispatcher April Florio and Sergeant Quon's wife, Jerilyn Quon, were using their own personal pagers but knew that Sergeant Quon's pager was issued by the Department. SER 303-04, 307. The panel opinion drew no distinctions among them, treating all three essentially as if they were third parties sending text messages to Sergeant Quon. As the United States pointed out, "[t]hough the panel stated that it did 'not endorse a monolithic view of text message users' reasonable expectation of privacy, as this is necessarily a context-sensitive inquiry,' the panel discussed few contextual facts other than whether Quon 'voluntarily permitted the Department to review his text messages.'" App., *infra*, 164-165 (quoting the panel opinion at App., *infra*, 28).

infra, 24-28. But whether users of text messaging *generally* have a reasonable expectation of privacy in the content of text messages is not the issue.[6] Neither the panel's reasoning nor the authorities it cited address a sender's expectation of privacy in communications sent to the recipient's *workplace* equipment – here a government employer's equipment.[7]

It is not objectively reasonable to expect privacy in a message sent to someone else's workplace pager, let alone to a police officer's department-issued pager. To have such an expectation, the sender would have to believe the recipient's employer does *not* have a no-privacy policy in place as to that employer's electronic communications equipment. That is *un*reasonable. As the United States aptly pointed out, "[n]ot only do

---

[6] In its amicus brief supporting rehearing en banc, the United States pointed out additional problems with the panel's categorical determination that all users of text messaging have a reasonable expectation that their messages are private. App., *infra*, 163-171. Foremost, the United States argued that the panel's ruling was erroneous "because it made categorical conclusions about entire modes of communication without considering all relevant circumstances," and that "the Sixth Circuit, en banc, had recently rejected a similarly sweeping categorical conclusion about the privacy of e-mail." App., *infra*, 163 (citing *Warshak v. United States*, 532 F.3d 521, 527 (6th Cir. 2008) (en banc). The United States also argued that there generally is no reasonable expectation of privacy in text messages sent and received. App., *infra*, 177-180.

[7] None of the cases involving telephone calls, letters, e-mails, or computer usage cited by panel even addressed government employer searches; they addressed law enforcement searches. *See* App., *infra*, 24-28.

senders lack knowledge of what privacy policy applies to a recipient, but few actions demonstrate an expectation of privacy less than transmission of information to the work account of a public employee charged with enforcing the law." App., *infra*, 179.

Most employers have explicit no-privacy policies. "[T]he abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible." *Muick*, 280 F.3d at 743; *see also TBG Ins. Servs. Corp. v. Superior Court*, 117 Cal. Rptr. 2d 155, 161-62, 96 Cal. App. 4th 443, 451 (2002) (finding no reasonable expectation of privacy in computer provided by employer for employee's home use and noting report that "more than three-quarters of this country's major firms monitor, record, and review employee communications and activities on the job, including their telephone calls, e-mails, Internet connections, and computer files").

In particular, "numerous government agencies," like the City of Ontario, have adopted "policies [that] typically require employees to acknowledge that their e-mail records are subject to inspection, monitoring, and public disclosure; that they have no right of privacy or any reasonable expectation of privacy in workplace e-mails; that the e-mails are owned by the agency, not the employee; and that e-mails are presumptively considered to be public records." Peter

S. Kozinets, *Access to the E-Mail Records of Public Officials: Safeguarding the Public's Right to Know*, 25-SUM Comm. Law. 17, 23 (2007). For example, the United States is "a public employer that extensively uses 'no confidentiality' policies with respect to the workplace and work-issued equipment." App., *infra*, 162.

The Ninth Circuit, however, ignored the prevalence of such policies. In fact, it even ignored the explicit policy in this case, concluding that "[h]ad Jeff Quon voluntarily permitted the Department to review his text messages, the remaining Appellants would have no claims." App., *infra*, 28. But Sergeant Quon *did* consent by signing the City's written policy.[8]

The panel failed to consider whether the senders' expectation of privacy is objectively reasonable for Fourth Amendment purposes in light of all these surrounding circumstances. Remarkably, the panel concluded that plaintiffs "prevail *as a matter of law*." App., *infra*, 40 (emphasis added). The panel's sweeping extension of Fourth Amendment protection threatens any government employer's ability to monitor even its *own* employees' electronic communications, which inevitably will include messages sent from third-party senders. The Ninth Circuit opinion thus further hamstrings public employers' ability to

---

[8] Again, the panel relied on Lieutenant Duke's informal policy only when it addressed whether *Sergeant Quon* had a reasonable expectation of privacy. App., *infra*, 27 n.6.

prevent abuse and protect the integrity of workplace communications.

IV. THIS CASE PRESENTS AN EXCELLENT VEHICLE TO ADDRESS *O'CONNOR*'S APPLICATION TO NEW WORKPLACE TECHNOLOGIES; THERE IS NO BASIS FOR THE FACTUAL CONCERNS POSITED BY THE OPINION CONCURRING IN THE DENIAL OF REHEARING EN BANC.

As we have explained, there is no merit to the concurring opinion's criticisms of the legal analysis provided by the opinion dissenting from the denial of rehearing en banc. The concurrence also takes the dissent to task for supposedly taking liberties with the facts of the case. App., *infra*, 125-131. But the record soundly refutes these criticisms as well. For example:

- The concurrence says "the record is clear that the City had no official policy governing the use of the pagers." App., *infra*, 127. But the panel opinion itself says that "Quon signed [the Department's general "Computer Usage, Internet and E-mail Policy"] and attended a meeting in which it was made clear that the Policy also *applied to use of the pagers*." App., *infra*, 29 (emphasis added); *see also* App., *infra*, 48 (district court noting meeting and also subsequent memorandum that memorialized meeting and was sent to

Sergeants Quon and Trujillo). What more does it take for a City to have an official policy governing pagers? As we discussed above, even the panel expressly acknowledged that the written policy would control if not for Lieutenant Duke's informal policy. App., *infra*, 29-30.[9]

- According to the concurrence, "[t]he record belies the dissent's assertion that the OPD officers were permitted to use the pagers only during SWAT emergencies." App., *infra*, 126. But the dissent did not make that assertion. Rather, the dissent said that the Department "obtained two-way pagers for its SWAT team members to enable better coordination, and more rapid and effective responses to emergencies," App., *infra*, 138; *see also* App., *infra*, 142, which not only comports with common sense but also is exactly what the district court found. App., *infra*, 45-46.

---

[9] The panel's reasoning suggests that government employees can use a newly-acquired technology however they please unless and until the employer issues a policy expressly covering it and that it is not enough to inform the employees that existing policies cover new technologies. This notion is antithetical to the reasonableness standard of the Fourth Amendment and to the special needs of government employers articulated in *O'Connor*.

- The concurrence says the dissent ignores the jury's finding that Chief Scharf's purpose in having Lieutenant Duke audit Sergeant Quon's pager messages was to determine the efficacy of the Department's existing character limits. App., *infra*, 130. But the dissent did acknowledge that Chief Scharf ordered the audit "to determine whether the police department's contract with their service provider was sufficient to meet its needs for text messaging." App., *infra*, 139-140 (citing the panel opinion). If anything, it was the panel that was reluctant to accept the jury's verdict on this issue, hypothesizing other ways "to verify the efficacy of the 25,000 character limit (*if that, indeed, was the intended purpose*)." App., *infra*, 35 (emphasis added).

- The concurrence chides the dissent for stating that "Chief Scharf 'sent the matter to internal affairs for an investigation "to determine if someone was wasting . . . City time not doing work when they should be."'" App., *infra*, 130. But the dissent's statement is nearly *identical* to what the panel opinion said: "Chief Scharf referred the matter to internal affairs 'to determine if someone was wasting . . . City time not doing work when they should be.'" App., *infra*, 9; *see also* App., *infra*, 55 (district court stating same).

And while the concurring opinion emphasizes that the panel's holding was "fact-driven," App., *infra*, 126, most Fourth Amendment cases are. As the concurrence itself later states, the *O'Connor* "analysis is necessarily fact-driven." App., *infra*, 132. That is no reason for this Court to turn a blind eye on a circuit court opinion that seriously undermines Fourth Amendment jurisprudence on issues of great importance.

CONCLUSION

The petition for a writ of certiorari should be granted. Because the Ninth Circuit's ruling manifestly contravenes this Court's Fourth Amendment precedents, the Court should consider summary reversal.

Respectfully submitted.

DIMITRIOS C. RINOS
Rinos & Martin, LLP
17862 East 17th Street, Suite 104
Tustin, California 92780
(714) 734-0400

KENT L. RICHLAND
(Counsel of Record)
KENT J. BULLARD
Greines, Martin, Stein & Richland LLP
5900 Wilshire Boulevard, 12th Floor
Los Angeles, California 90036
(310) 859-7811

Counsel for Petitioners

APRIL 2009

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. LORI DREW, Defendant.	No. CR 08-0582-GW DECISION ON DEFENDANT'S F.R.CRIM.P. 29(c) MOTION

I. INTRODUCTION

This case raises the issue of whether (and/or when will) violations of an Internet website's[1] terms of service constitute a crime under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. Originally, the question arose in the context of Defendant Lori Drew's motions to dismiss the Indictment on grounds of vagueness, failure to state an offense, and unconstitutional delegation of prosecutorial power. See Case Docket Document Numbers ("Doc. Nos.") 21, 22, and 23. At that time, this Court found that the presence of the scienter element (i.e. the requirement that the intentional accessing of a computer without authorization or in excess of authorization

[1] There is some disagreement as to whether the words "Internet" and "website" should be capitalized and whether the latter should be two words (i.e. "web site") or one. "Internet" is capitalized as that is how the word appears most often in Supreme Court opinions. See, e.g., Pac. Bell Tel. Co. v. linkline Comms., Inc., 555 U.S. ___, 129 S.Ct. 1109, 1115 (2009).

be in furtherance of the commission of a criminal or tortious act) within the CFAA felony provision as delineated in 18 U.S.C. § 1030(c)(2)(B)(ii) overcame Defendant's constitutional challenges and arguments against the criminalization of breaches of contract involving the use of computers. See Reporter's Transcripts of Hearings on September 4 and October 30, 2008. However, Drew was subsequently acquitted by a jury of the felony CFAA counts but convicted of misdemeanor CFAA violations. Hence, the question in the present motion under Federal Rule of Criminal Procedure ("F.R.Crim.P.") 29(c) is whether an intentional breach of an Internet website's terms of service, without more, is sufficient to constitute a misdemeanor violation of the CFAA; and, if so, would the statute, as so interpreted, survive constitutional challenges on the grounds of vagueness and related doctrines.[2]

II. BACKGROUND

A. Indictment

In the Indictment, Drew was charged with one count of conspiracy in violation of 18 U.S.C. § 371 and three counts of violating a felony portion of the CFAA, i.e., 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), which prohibit accessing a computer without authorization or in excess of authorization and obtaining information

---

[2] While this case has been characterized as a prosecution based upon purported "cyberbulling," there is nothing in the legislative history of the CFAA which suggests that Congress ever envisioned such an application of the statute. See generally, A. Hugh Scott & Kathleen Shields, Computer and Intellectual Property Crime: Federal and State Law (2006 Cumulative Supplement) 4-8 to 4-16 (BNA Books 2006). As observed in Charles Doyle & Alyssa Weir, CRS Report for Congress - Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws (Order Code 97-1025) (Updated June 28, 2005):

> The federal computer fraud and abuse statute, 18 U.S.C. 1030, protects computers in which there is a federal interest – federal computers, bank computers, and computers used in interstate and foreign commerce. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, instead it fills cracks and gaps in the protection afforded by other state and federal criminal laws.

Moreover, once Drew was acquitted by the jury of unauthorized accessing of a protected computer in furtherance of the commission of acts of intentional infliction of emotional distress, this case was no longer about "cyberbulling" (if, indeed, it was ever properly characterized as such); but, rather, it concerned the proper scope of the application of the CFAA in the context of violations of a website's terms of service.

from a protected computer where the conduct involves an interstate or foreign communication and the offense is committed in furtherance of a crime or tortious act. See Doc. No. 1.

The Indictment included, inter alia, the following allegations (not all of which were established by the evidence at trial). Drew, a resident of O'Fallon, Missouri, entered into a conspiracy in which its members agreed to intentionally access a computer used in interstate commerce without (and/or in excess of) authorization in order to obtain information for the purpose of committing the tortious act of intentional infliction of emotional distress[3] upon "M.T.M.," subsequently identified as Megan Meier ("Megan"). Megan was a 13 year old girl living in O'Fallon who had been a classmate of Drew's daughter Sarah. Id. at ¶¶ 1- 2, 14. Pursuant to the conspiracy, on or about September 20, 2006, the conspirators registered and set up a profile for a fictitious 16 year old male juvenile named "Josh Evans" on the www.MySpace.com website ("MySpace"), and posted a photograph of a boy without that boy's knowledge or consent. Id. at ¶ 16. Such conduct violated MySpace's terms of service. The conspirators contacted Megan through the MySpace network (on which she had her own profile) using the Josh Evans pseudonym and began to flirt with her over a number of days. Id. On or about October 7, 2006, the conspirators had "Josh" inform Megan that he was moving away. Id. On or about October 16, 2006, the conspirators had "Josh" tell Megan that he no longer liked her and that "the world would be a better place without her in it." Id. Later on that same day, after learning that Megan had killed herself, Drew caused the Josh Evans MySpace account to be deleted. Id.

---

[3] The elements of the tort of intentional infliction of emotional distress are the same under both Missouri and California state laws. Those elements are: (1) the defendant must act intentionally or recklessly; (2) the defendant's conduct must be extreme or outrageous; and (3) the conduct must be the cause (4) of extreme emotional distress. See, e.g., Thomas v. Special Olympics Missouri, Inc., 31 S.W.3d 442, 446 (Mo. Ct. App. 2000); Hailey v. California Physicians' Service, 158 Cal.App.4th 452, 473-74 (2007).

B. Verdict

At the trial, after consultation between counsel and the Court, the jury was instructed that, if they unanimously decided that they were not convinced beyond a reasonable doubt as to the Defendant's guilt as to the felony CFAA violations of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), they could then consider whether the Defendant was guilty of the "lesser included"[4] misdemeanor CFAA violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A).[5]

At the end of the trial, the jury was deadlocked and was unable to reach a verdict as to the Count 1 conspiracy charge.[6] See Doc. Nos. 105 and 120. As to Counts 2 through 4, the jury unanimously found the Defendant "not guilty" "of [on

---

[4] As provided in F.R.Crim.P. 31(c)(1), a "defendant may be found guilty of . . . an offense necessarily included in the offense charged . . . ." A "lesser included" crime is one where "the elements of the lesser offense are a subset of the elements of the charged offense." Carter v. United States, 530 U.S. 255, 260 (2000) (quoting Schmuck v. United States, 489 U.S. 705, 716 (1989)). Because the felony CFAA crime in 18 U.S.C. § 1030(c)(2)(B)(ii) consists of committing acts which constitute a violation of the misdemeanor CFAA crime in 18 U.S.C. § 1030(a)(2)(C) (as delineated in 18 U.S.C. § 1030(c)(2)(A)) plus the additional element that the acts were done "in furtherance of any crime or tortious act in violation of the Constitution or laws of the United States or any State," the misdemeanor CFAA crime is a "lesser included" offense as to the felony CFAA violation.

A defendant is entitled to a "lesser included" offense jury instruction if the evidence warrants it. Guam v. Fejeran, 687 F.2d 302, 305 (9th Cir. 1982).

[5] Specifically, the jury was instructed that:

> The crime of accessing a protected computer without authorization or in excess of authorization to obtain information, and to do so in furtherance of a tortious act in violation of the laws of any State, includes the lesser crime of accessing a protected computer without authorization or in excess of authorization. If (1) all of you are not convinced beyond a reasonable doubt that the defendant is guilty of accessing a protected computer without authorization or in excess of authorization to obtain information, and doing so in furtherance of a tortious act in violation of the laws of any State; and (2) all of you are convinced beyond a reasonable doubt that the defendant is guilty of the lesser crime of accessing a protected computer without authorization or in excess of authorization, you may find the defendant guilty of accessing a protected computer without authorization or in excess of authorization.

See Jury Instruction No. 24, Doc. No. 107.

[6] The conspiracy count was subsequently dismissed without prejudice at the request of the Government.

the dates specified in the Indictment] accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information in furtherance of the tort of intentional infliction of emotional distress in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(ii) . . . ." Id. The jury did find Defendant "guilty" "of [on the dates specified in the Indictment] accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(A), a misdemeanor." Id.

C. MySpace.com

As Jae Sung (Vice President of Customer Care at MySpace) ("Sung") testified at trial, MySpace is a "social networking" website where members can create "profiles" and interact with other members. See Reporter's Transcript of the November 21, 2008 Sung testimony ("11/21/08 Transcript") at pages 40-41. Anyone with Internet access can go onto the MySpace website and view content which is open to the general public such as a music area, video section, and members' profiles which are not set as "private." Id. at 42. However, to create a profile, upload and display photographs, communicate with persons on the site, write "blogs," and/or utilize other services or applications on the MySpace website, one must be a "member." Id. at 42-43. Anyone can become a member of MySpace at no charge so long as they meet a minimum age requirement and register. Id.

In 2006, to become a member, one had to go to the sign-up section of the MySpace website and register by filling in personal information (such as name, email address, date of birth, country/state/postal code, and gender) and creating a password. Id. at 44-45. In addition, the individual had to check on the box indicating that "You agree to the MySpace **Terms of Service** and **Privacy Policy**." See Government's[7]

[7] All exhibits referenced herein were proffered by the Government and admitted during the trial.

Exhibit 1 at page 2 (emphasis in original); 11/21/08 Transcript at 45-47. The terms of service did not appear on the same registration page that contained this "check box" for users to confirm their agreement to those provisions. Id. In order to find the terms of service, one had (or would have had) to proceed to the bottom of the page where there were several "hyperlinks" including one entitled "Terms." 11/21/08 Transcript at 50; Exhibit 1 at 5. Upon clicking the "Terms" hyperlink, the screen would display the terms of service section of the website. Id. A person could become a MySpace member without ever reading or otherwise becoming aware of the provisions and conditions of the MySpace terms of service by merely clicking on the "check box" and then the "Sign Up" button without first accessing the "Terms" section. 11/21/08 Transcript at 94.[8]

As used in its website, "terms of service" refers to the "MySpace.com Terms of Use Agreement" ("MSTOS"). See Government's Exhibit 3. The MSTOS in 2006 stated, inter alia:

> This Terms of Use Agreement ("Agreement") sets forth the legally binding terms for your use of the Services. By using the Services, you agree to be bound by this Agreement, whether you are a "Visitor" (which means that you simply browse the Website) or you are a "Member" (which means that you have registered with Myspace.com). The term "User" refers to a Visitor or a Member. You are only authorized to use the Services (regardless of whether your access or use is intended) if you agree to abide by all applicable laws and to this Agreement. Please read this Agreement carefully and save it. If you do not agree with it, you should leave the Website and discontinue use of the Services immediately. If you wish to become a Member, communicate with other Members and make use of the Services, you must read this Agreement and indicate your acceptance at the end of this document before proceeding.

Id. at 1.

---

[8] Certain websites endeavor to compel visitors to read their terms of service by requiring them to scroll down through such terms before being allowed to click on the sign-on box or by placing the box at the end of the "terms" section of the site. Id. at 93. MySpace did not have such provisions in 2006. Id. See generally Southwest Airlines, Co. v. BoardFirst, L.L.C., 2007 U.S. Dist. LEXIS 96230 at *13-16 & n.4 (N.D. Tex. 2007) (discussing various methods that websites employ to notify users of terms of service).

> By using the Services, you represent and warrant that (a) all registration information you submit is truthful and accurate; (b) you will maintain the accuracy of such information; (c) you are 14 years of age or older; and (d) your use of the Services does not violate any applicable law or regulation.

Id. at 2.

The MSTOS prohibited the posting of a wide range of content on the website including (but not limited to) material that: a) "is potentially offensive and promotes racism, bigotry, hatred or physical harm of any kind against any group or individual"; b) "harasses or advocates harassment of another person"; c) "solicits personal information from anyone under 18"; d) "provides information that you know is false or misleading or promotes illegal activities or conduct that is abusive, threatening, obscene, defamatory or libelous"; e) "includes a photograph of another person that you have posted without that person's consent"; f) "involves commercial activities and/or sales without our prior written consent"; g) "contains restricted or password only access pages or hidden pages or images"; or h) "provides any phone numbers, street addresses, last names, URLs or email addresses . . . ." Id. at 4. MySpace also reserved the right to take appropriate legal action (including reporting the violating conduct to law enforcement authorities) against persons who engaged in "prohibited activity" which was defined as including, inter alia: a) "criminal or tortious activity", b) "attempting to impersonate another Member or person", c) "using any information obtained from the Services in order to harass, abuse, or harm another person", d) "using the Service in a manner inconsistent with any and all applicable laws and regulations", e) "advertising to, or solicitation of, any Member to buy or sell any products or services through the Services", f) "selling or otherwise transferring your profile", or g) "covering or obscuring the banner advertisements on your personal profile page . . . ." Id. at 5. The MSTOS warned users that "information provided by other MySpace.com Members (for instance, in their Profile) may contain inaccurate, inappropriate, offensive or sexually explicit material, products or services, and MySpace.com assumes no responsibility or liability for this material." Id. at 1-2.

Further, MySpace was allowed to unilaterally modify the terms of service, with such modifications taking effect upon the posting of notice on its website. Id. at 1. Thus, members would have to review the MSTOS each time they logged on to the website, to ensure that they were aware of any updates in order to avoid violating some new provision of the terms of service. Also, the MSTOS provided that "any dispute" between a visitor/member and MySpace "arising out of this Agreement must be settled by arbitration" if demanded by either party. Id. at 7.

At one point, MySpace was receiving an estimated 230,000 new accounts per day and eventually the number of profiles exceeded 400 million with over 100 million unique visitors worldwide. 11/21/08 Transcript at 74-75. "Generally speaking," MySpace would not monitor new accounts to determine if they complied with the terms of service except on a limited basis, mostly in regards to photographic content. Id. at 75. Sung testified that there is no way to determine how many of the 400 million existing MySpace accounts were created in a way that violated the MSTOS.[9] Id. at 82-84. The MySpace website did have hyperlinks labelled "Safety Tips" (which contained advice regarding personal, private and financial security vis-a-vis the site) and "Report Abuse" (which allowed users to notify MySpace as to inappropriate content and/or behavior on the site). Id. at 51-52. MySpace attempts to maintain adherence to its terms of service. Id. at 60. It has different teams working in various areas such as "parent care" (responding to parents' questions about this site), handling "harassment/cyberbully cases, imposter profiles," removing inappropriate content, searching for underage users, etc. Id. at 60-61. As to MySpace's response to reports

---

[9] As stated in the MSTOS:

> MySpace.com does not endorse and has no control over the Content. Content is not necessarily reviewed by MySpace.com prior to posting and does not necessarily reflect the opinions or policies of MySpace.com. MySpace.com makes no warranties, express or implied, as to the Content or to the accuracy and reliability of the Content or any material or information that you transmit to other Members.

Exhibit 3 at 3.

of harassment:

> It varies depending on the situation and what's being reported. It can range from . . . letting the user know that if they feel threatened to contact law enforcement, to us removing the profile, and in rare circumstances we would actually contact law enforcement ourselves.

Id. at 61.

Once a member is registered and creates his or her profile, the data is housed on computer servers which are located in Los Angeles County. Id. at 53. Members can create messages which can be sent to other MySpace members, but messages cannot be sent to or from other Internet service providers such as Yahoo!. Id. at 54. All communications among MySpace members are routed from the sender's computer through the MySpace servers in Los Angeles. Id. at 54-55.

Profiles created by adult MySpace members are by default available to any user who accesses the MySpace website. Id. at 56. The adult members can, however, place privacy settings on their accounts such that only pre-authorized "friends" are able to view the members' profile pages and contents. Id. For members over 16 but under 18, their profiles are by default set at "private" but can be changed by the member. Id. at 57. Members under 16 have a privacy setting for their profiles which cannot be altered to allow regular public access. Id. To communicate with a member whose profile has a privacy setting, one must initially send a "friend" request to that person who would have to accept the request. Id. at 57-58. To become a "friend" of a person under 16, one must not only send a "friend" request but must also know his or her email address or last name. Id. at 58.

According to Sung, MySpace owns the data contained in the profiles and the other content on the website.[10] MySpace is owned by Fox Interactive Media which

---

[10] Technically, as delineated in the MSTOS, Exhibit 3 at pages 2-3:

> By displaying or publishing ("posting") any Content, messages, text, files, images, photos, video, sounds, profiles, works or authorship, or any other materials (collectively, "Content") on or through the Services, you hereby

is part of News Corporation. Id. at 42.

III. APPLICABLE LAW

A. F.R.Crim.P. 29(c)

A motion for judgment of acquittal under F.R.Crim.P. 29(c) may be made by a defendant seeking to challenge a conviction on the basis of the sufficiency of the evidence, see, e.g., United States v. Freter, 31 F.3d 783, 785 (9th Cir. 1994), or on other grounds including ones involving issues of law for the court to decide, see, e.g. United States v. Pardue, 983 F.2d 843, 847 (8th Cir. 1993) (issue as to whether a defendant is entitled to a judgment of acquittal based on outrageous government conduct is "one of law for the court"). Where the Rule 29(c) motion rests in whole or in part on the sufficiency of the evidence, the evidence must be viewed "in the light most favorable to the government" (see Freter, 31 F.3d at 785), with circumstantial evidence and inferences drawn in support of the jury's verdict. See United States v. Lewis, 787 F.2d 1318, 1323 (9th Cir. 1986).

B. The CFAA

In 2006, the CFAA (18 U.S.C. § 1030) provided in relevant part that:

> (a) Whoever –
>
> * * * *
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

---

grant to MySpace.com, a non-exclusive, fully-paid and royalty-free, worldwide license (with the right to sublicense through unlimited levels of sublicensees) to use, copy, modify, adapt, translate, publicly perform, publicly display, store, reproduce, transmit, and distribute such Content on and through the Services. This license will terminate at the time you remove such Content from the Services. Notwithstanding the foregoing, a back-up or residual copy of the Content posted by you may remain on the MySpace.com servers after you have removed the Content from the Services, and MySpace.com retains the rights to those copies.

> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer if the conduct involved an interstate or foreign communication;[11]
>
> * * * *
>
> shall be punished as provided in subsection (c) of this section.
>
> * * * *
>
> (c) The punishment for an offense under subsection (a) or (b) of this section is –
>
> * * * *
>
> (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; . . .
>
> (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if –
>
> (i) the offense was committed for purposes of commercial advantage or private financial gain;
>
> (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
>
> (iii) the value of the information obtained exceeds $5,000 . . . .

As used in the CFAA, the term "computer" "includes any data storage facility or communication facility directly related to or operating in conjunction with such device . . . ." 18 U.S.C. § 1030(e)(1). The term "protected computer" "means a computer - (A) exclusively for the use of a financial institution or the United States Government . . . ; or (B) which is used in interstate or foreign commerce or communication . . . ." Id. § 1030(e)(2). The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter . . .

---

[11] On September 26, 2008, the Identity Theft Enforcement and Restitution Act of 2008 was passed which amended 18 U.S.C. § 1030(a)(2)(C) by inter alia striking the words "if the conduct involved an interstate or foreign communication" after "protected computer." See 110 P.L. 326, Title II, § 203, 112 Stat. 3560-65.

." Id. § 1030(e)(6).

In addition to providing criminal penalties for computer fraud and abuse, the CFAA also states that "[A]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). Because of the availability of civil remedies, much of the law as to the meaning and scope of the CFAA has been developed in the context of civil cases.

IV. DISCUSSION

A. The Misdemeanor 18 U.S.C. § 1030(a)(2)(C) Crime Based on Violation of a Website's Terms of Service

During the relevant time period herein,[12] the misdemeanor 18 U.S.C. § 1030(a)(2)(C) crime consisted of the following three elements:

> First, the defendant intentionally [accessed without authorization] [exceeded authorized access of] a computer;
>
> Second, the defendant's access of the computer involved an interstate or foreign communication; and
>
> Third, by [accessing without authorization] [exceeding authorized access to] a computer, the defendant obtained information from a computer . . . [used in interstate or foreign commerce or communication] . . . .

Ninth Circuit Model Criminal Jury Instruction 8.79 (2003 Ed.) (brackets in original).

In this case, a central question is whether a computer user's intentional violation of one or more provisions in an Internet website's terms of services (where those terms condition access to and/or use of the website's services upon agreement to and compliance with the terms) satisfies the first element of section 1030(a)(2)(C). If the answer to that question is "yes," then seemingly, any and every conscious violation of that website's terms of service will constitute a CFAA misdemeanor.

Initially, it is noted that the latter two elements of the section 1030(a)(2)(C)

---

[12] See footnote 11, supra.

crime will always be met when an individual using a computer contacts or communicates with an Internet website. Addressing them in reverse order, the third element requires "obtain[ing] information" from a "protected computer" - which is defined in 18 U.S.C. § 1030(e)(2)(B) as a computer "which is used in interstate or foreign commerce or communication . . . ." "Obtain[ing] information from a computer" has been described as "'includ[ing] mere observation of the data. Actual aspiration . . . need not be proved in order to establish a violation . . . .' S.Rep. No. 99-432, at 6-7 (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2484." Comment, Ninth Circuit Model Criminal Instructions 8.77.[13] As for the "interstate or foreign commerce or communication" component, the Supreme Court in Reno v. American Civil Liberties Union, 521 U.S. 844, 849 (1997), observed that: "The Internet is an international network of interconnected computers." See also Brookfield Communications v. West Coast Entertainment Corp., 174 F.3d 1036, 1044 (9th Cir. 1999) ("The Internet is a global network of interconnected computers which allows individuals and organizations around the world to communicate and to share information with one another."). The Ninth Circuit in United States v. Sutcliffe, 505 F.3d 944, 952 (9th Cir. 2007), found the Internet to be "similar to - and often using - our national network of telephone lines." It went on to conclude that:

> We have previously agreed that "[i]t can not be questioned that the nation's vast network of telephone lines constitutes interstate commerce," United States v. Holder, 302 F.Supp. 296, 298 (D. Mont. 1969)), aff'd and adopted, 427 F.2d 715 (9th Cir. 1970) (per curiam), and, a fortiori, it seems clear that use of the internet is intimately related to interstate commerce. As we have noted, "[t]he Internet engenders a medium of communication that enables information to be quickly, conveniently, and inexpensively disseminated to hundreds of millions of individuals worldwide." United States v. Pirello, 255 F.3d 728, 729 (9th Cir. 2001). It is "comparable . . . to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and

[13] As also stated in Senate Report No. 104-357, at 7 (1996), reprinted at 1996 WL 492169 (henceforth "S. Rep. No. 104-357"), ". . . the term 'obtaining information' includes merely reading it."

> services," ACLU, 521 U.S. at 853, and is "a valuable tool in today's commerce," Pirello, 255 F.3d at 730. We are therefore in agreement with the Eighth Circuit's conclusion that "[a]s both the means to engage in commerce and the method by which transactions occur, "the Internet is an instrumentality and channel of interstate commerce." United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (per curiam) (quoting United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006)).

Id. at 952-53. Thus, the third element is satisfied whenever a person using a computer contacts an Internet website and reads any response from that site.

As to the second element (i.e., that the accessing of the computer involve an interstate or foreign communication),[14] an initial question arises as to whether the communication itself must be interstate or foreign (i.e., it is transmitted across state lines or country borders) or whether it simply requires that the computer system, which is accessed for purposes of the communication, is interstate or foreign in nature (for example, akin to a national telephone system).[15] The term "interstate or foreign communication" is not defined in the CFAA. However, as observed in Patrick Patterson Custom Homes, Inc. v. Bach, 586 F.Supp.2d 1026, 1033 (N.D. Ill. 2008), "[t]he plain language of section 1030(a)(2)(C) requires that the conduct of unlawfully accessing a computer, and not the obtained information, must involve an interstate or foreign communication." See also Charles Schwab & Co. Inc. v. Carter, 2005 U.S. Dist. LEXIS 21348 at *26 (N.D. Ill. 2005). It has been held that "[a]s a practical matter, a computer providing a 'web-based' application accessible through the internet would satisfy the 'interstate communication' requirement." Paradigm Alliance, Inc. v. Celeritas Technologies, LLC, 248 F.R.D. 598, 602 (D. Kan. 2008); see also Patrick

---

[14] It is noted that, with the 2008 amendment to section 1030(a)(2)(C) which struck the provision that "the conduct involved an interstate or foreign communication" (see footnote 11, supra), the second element is no longer a requirement for the CFAA 18 U.S.C. § 1030(a)(2)(C) crime, although the interstate/foreign nexus remains as part of the third element.

[15] A resolution of that question would not effect Defendant's conviction here since the undisputed evidence at trial is that MySpace's server is connected to the Internet and the communications made by the alleged conspirators in O'Fallon, Missouri to Megan would automatically be routed to MySpace's server in Beverly Hills, California where it would be stored and thereafter sent to or retrieved by Megan in O'Fallon.

Patterson Custom Homes, 586 F.Supp.2d at 1033-34; Modis, Inc. v. Bardelli, 531 F.Supp.2d 314, 318-19 (D. Conn. 2008); Charles Schwab & Co., 2005 U.S. Dist. LEXIS 21348 at *26-27. This interpretation is consistent with the legislative history of the CFAA.[16] Therefore, where contact is made between an individual's computer and an Internet website, the second element is per se established.

As to the first element (i.e. intentionally accessing a computer without authorization or exceeding authorized access), the primary question here is whether any conscious violation of an Internet website's terms of service will cause an individual's contact with the website via computer to become "intentionally access[ing] . . . without authorization" or "exceeding authorization." Initially, it is noted that three of the key terms of the first element (i.e., "intentionally," "access a computer," and "without authorization") are undefined, and there is a considerable amount of controversy as to the meaning of the latter two phrases. See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive."); Southwest Airlines Co. v. BoardFirst, L.L.C., 2007 U.S. Dist. LEXIS 96230 at *36 (N.D. Tex. 2007) ("BoardFirst") ("The CFAA does not define the term 'access'."); Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse

---

[16] For example, as stated in S. Rep. No. 104-357, at 13:

> The bill would amend subsection 1030(e)(2) by replacing the term "Federal interest computer" with the new term "protected computer" and a new definition . . . . The new definition also replaces the current limitation in subsection 1030(e)(2)(B) of "Federal interest computer" being "one of two or more computers used in committing the offense, not all of which are located in the same State." Instead, "protected computer" would include computers "used in interstate or foreign commerce or communications." Thus, hackers who steal information or computer usage from computers in their own State would be subject to this law, under amended section 1030(a)(4), if the requisite damage threshold is met and the computer is used in interstate commerce or foreign commerce or communications.

Statutes, 78 N.Y.U. L. Rev. 1596, 1619-21 (2003) ("Kerr, Cybercrime's Scope"); Mark A. Lemley, Place and Cyberspace, 91 Cal. L. Rev. 521, 528-29 (2003); Dan Hunter, Cyberspace as Place and the Tragedy of the Digital Anticommons, 91 Cal. L. Rev. 439, 477 (2003).

While "intentionally" is undefined, the legislative history of the CFAA clearly evinces Congress's purpose in its choice of that word. Prior to 1986, 18 U.S.C. § 1030(a)(2) utilized the phrase "knowingly accesses." See United States Code 1982 Ed. Supp. III at 16-17. In the 1986 amendments to the statute, the word "intentionally" was substituted for the word "knowingly." See 18 U.S.C.A. § 1030 "Historical and Statutory Notes" at 450 (West 2000). In Senate Report No. 99-432 at 5-6, reprinted at 1986 U.S.C.C.A.N. 2479, 2483-84, it was stated that:

> Section 2(a)(1) amends 18 U.S.C. 1030(a)(2) to change the scienter requirement from "knowingly" to "intentionally," for two reasons. First, intentional acts of unauthorized access - rather than mistaken, inadvertent, or careless ones - are precisely what the Committee intends to proscribe. Second, the Committee is concerned that the "knowingly" standard in the existing statute might be inappropriate for cases involving computer technology . . . . The substitution of an "intentional" standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another. Again, this will comport with the Senate Report on the Criminal Code, which states that "'intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective." [Footnote omitted.]

Under § 1030(a)(2)(C), the "requisite intent" is "to obtain unauthorized access of a protected computer." United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007) ("The government need not also prove that . . . the information was used to any particular ends."); see also S.Rep. No.104-357, at 7-8 ("[T]he crux of the offense under subsection 1030(a)(2)(C) . . . is abuse of a computer to obtain the information.").

As to the term "accesses a computer," one would think that the dictionary definition of verb transitive "access" would be sufficient. That definition is "to gain

or have access to; to retrieve data from, or add data to, a database . . . ." Webster's New World Dictionary, Third College Edition, 7 (1988) (henceforth "Webster's New World Dictionary"). Most courts that have actually considered the issue of the meaning of the word "access" in the CFAA have basically turned to the dictionary meaning. See e.g. BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *36; Role Models Am., Inc. v. Jones, 305 F. Supp. 2d 564, 566-57 (D. Md. 2004); Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 121 F.Supp.2d 1255, 1272-73 (N.D. Iowa 2000). However, academic commentators have generally argued for a different interpretation of the word. For example, as stated in Patricia L. Bellia, Defending Cyberproperty, 79 N.Y.U. L. Rev. 2164, 2253-54 (2004):

> We can posit two possible readings of the term "access." First, it is possible to adopt a broad reading, under which "access" means any interaction between two computers. In other words, "accessing" a computer simply means transmitting electronic signals to a computer that the computer processes in some way. A narrower understanding of "access" would focus not merely on the successful exchange of electronic signals, but rather on conduct by which one is in a position to obtain privileges or information not available to the general public. The choice between these two meanings of "access" obviously affects what qualifies as unauthorized conduct. If we adopt the broader reading of access, and any successful interaction between computers qualifies, then breach of policies or contractual terms purporting to outline permissible uses of a system can constitute unauthorized access to the system. Under the narrower reading of access, however, only breach of a code-based restriction on the system would qualify.

Professor Bellia goes on to conclude that "[c]ourts would better serve both the statutory intent of the CFAA and public policy by limiting its application to unwanted uses only in connection with code-based controls on access." Id. at 2258. But see Kerr, Cybercrime's Scope, 78 N.Y.U. L. Rev. at 1619-21, 1643, and 1646-48 (arguing for a "broad construction of access . . . . as any successful interaction with the computer"). It is simply noted that, while defining "access" in terms of a code-based

restriction might arguably be a preferable approach, no case has adopted it[17] and the CFAA legislative history does not support it.

As to the term "without authorization," the courts that have considered the phrase have taken a number of different approaches in their analysis. See generally Kerr, Cybercrime's Scope, 78 N.Y.U. L. Rev. at 1628-40. Those approaches are usually based upon analogizing the concept of "without authorization" as to computers to a more familiar and mundane predicate presented in or suggested by the specific factual situation at hand. See e.g. United States v. Phillips, 477 F.3d 215, 219 (5th Cir.), cert. denied, 128 S.Ct. 119 (2007), ("Courts have therefore typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user."). Thus, for example, where a case arises in the context of employee misconduct, some courts have treated the issue as falling within an agency theory of authorization. See, e.g., International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1124-25 (W.D. Wash. 2000). Likewise, the Ninth Circuit (in dealing with the issue of purported consent to access emails pursuant to a subpoena obtained in bad faith in the context of the Stored Communications Act, 18 U.S.C. § 2701 et seq., and the CFAA) applied the law of trespass to determine whether a subpoenaed party had effectively authorized the defendants' access. See Theofel v. Farey-Jones, 359 F.3d 1066, 1072-75, 1078 (9th Cir. 2004). Further, where the relationship between the parties is contractual in nature or resembles such a relationship, access has been held to be unauthorized where there has been an ostensible breach of contract. See e.g., EF Cultural Travel BV, 274 F.3d at 583-84; Phillips, 477 F.3d at 221 ("[c]ourts have

---

[17] But see BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *43-44 ("§ 1030(a)(2)(C). However, the BoardFirst court did not adopt a "code-based" definition of "accessing without authorization" but requested further briefing on the issue.

recognized that authorized access typically arises only out of a contractual or agency relationship."). But see Brett Senior & Associates v. Fitzgerald, 2007 U.S. Dist. LEXIS 50833 at *13-14 (E.D. Pa. 2007) (observing - in the context of an employee's breach of a confidentiality agreement when he copied information from his firm's computer files to give to his new employer: "It is unlikely that Congress, given its concern 'about the appropriate scope of Federal jurisdiction' in the area of computer crime, intended essentially to criminalize state-law breaches of contract.").

Within the breach of contract approach, most courts that have considered the issue have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization. See, e.g., Southwest Airlines Co. v. Farechase, Inc., 318 F.Supp.2d 435, 439-40 (N.D. Tex. 2004); Nat'l Health Care Disc., Inc., 174 F.Supp.2d at 899; Register.com, Inc. v. Verio, Inc., 126 F.Supp.2d 238, 247-51 (S.D.N.Y. 2000), aff'd, 356 F.3d 393 (2d Cir. 2004); Am. Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444, 450 (E.D. Va. 1998); see also EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62-63 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access . . . . [W]e think that the public website provider can easily spell out explicitly what is forbidden . . . ."). But see BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *40 (noting that the above cases and their particular application of the law "have received their share of criticism from commentators"). The court in BoardFirst further stated:

> [I]t is at least arguable here that BoardFirst's access of the Southwest website is not at odds with the site's intended function; after all, the site is designed to allow users to obtain boarding passes for Southwest flights via the computer. In no sense can BoardFirst be considered an "outside hacker[] who break[s] into a computer" given that southwest.com is a publicly available website that anyone can access and use. True, the Terms posted on southwest.com do not give sanction to the particular *manner* in which BoardFirst uses the site -- to check in Southwest customers for financial gain. But then again § 1030 (a)(2)(C) does not forbid the *use* of a protected computer

> for any prohibited *purpose*; instead it prohibits one from intentionally *accessing* a computer "without authorization". As previously explained, the term "access", while not defined by the CFAA, ordinarily means the "freedom or ability to . . . make use of" something. Here BoardFirst or any other computer user obviously has the *ability* to make use of southwest.com given the fact that it is a publicly available website the access to which is not protected by any sort of code or password. *Cf.* Am. Online, 121 F.Supp.2d at 1273 (remarking that it is unclear whether an AOL member's violation of the AOL membership agreement results in "unauthorized access").[18]

Id. at 43-44 (emphasis in original).

In this particular case, as conceded by the Government,[19] the only basis for finding that Drew intentionally accessed MySpace's computer/servers without authorization and/or in excess of authorization was her and/or her co-conspirator's violations of the MSTOS by deliberately creating the false Josh Evans profile, posting a photograph of a juvenile without his permission and pretending to be a sixteen year old O'Fallon resident for the purpose of communicating with Megan. Therefore, if conscious violations of the MySpace terms of service were not sufficient to satisfy the first element of the CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(b)(2)(A), Drew's Rule 29(c) motion would have to be granted on that basis alone. However, this Court concludes that an intentional breach of the MSTOS can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the statute.

There is nothing in the way that the undefined words "authorization" and "authorized" are used in the CFAA (or from the CFAA's legislative history[20]) which

---

[18] Subsequently, the court in Am. Online did conclude that violating the website's terms of service would be sufficient to constitute "exceed[ing] authorized access." 174 F.Supp.2d at 899.

[19] See Reporter's Transcript of July 2, 2009 Hearing at 3-4.

[20] For example, when Congress added the term "exceeds authorized access" to the CFAA in 1986 and defined it as meaning "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter", it was observed that the definition (which includes the concept of accessing a computer with authorization) was "self-explanatory."

indicates that Congress intended for them to have specialized meanings.[21] As delineated in Webster's New World Dictionary at 92, to "authorize" ordinarily means "to give official approval to or permission for . . . ."

It cannot be considered a stretch of the law to hold that the owner of an Internet website has the right to establish the extent to (and the conditions under) which members of the public will be allowed access to information, services and/or applications which are available on the website. See generally Phillips, 477 F.3d at 219-21; EF Cultural Travel BV, 318 F.3d at 62; Register.com, Inc., 126 F.Supp.2d at 245-46; CompuServe Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015, 1023-24 (S.D. Ohio 1997). Nor can it be doubted that the owner can relay and impose those limitations/restrictions/conditions by means of written notice such as terms of service or use provisions placed on the home page of the website. See EF Cultural Travel BV, 318 F.3d at 62-63. While issues might be raised in particular cases as to the sufficiency of the notice and/or sufficiency of the user's assent to the terms, see generally Specht v. Netscape Communications Corp., 306 F.3d 17, 30-35 (2d Cir. 2002); BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *11-21, and while public policy considerations might in turn limit enforcement of particular restrictions, see EF Cultural Travel BV, 318 F.3d at 62, the vast majority of the courts (that have considered the issue) have held that a website's terms of service/use can define what is (and/or is not) authorized access vis-a-vis that website.

Here, the MSTOS defined "services" as including "the MySpace.com Website . . . , the MySpace.com instant messenger, and any other connection with the Website . . . ." See Exhibit 3 at 1. It further notified the public that the MSTOS "sets forth the

---

See S.Rep. No. 99-432, at 13 (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2491.

[21] Commentators have criticized the legislatures' understandings of computers and the accessing of computers as "simplistic" and based upon the technology in existence in the 1970's and 1980's (e.g. pre-Internet) rather than upon what currently exists. See, e.g., Kerr, Cybercrime's Scope, 78 N.Y.U. L. Rev. at 1640-41.

legally binding terms for your use of the services." Id. Visitors and members were informed that "you are only authorized to use the Services . . . if you agree to abide by all applicable laws and to this Agreement." Id. Moreover, to become a MySpace member and thereby be allowed to communicate with other members and fully utilize the MySpace Services, one had to click on a box to confirm that the user had agreed to the MySpace Terms of Service. Id.; see also Exhibit 1 at 2. Clearly, the MSTOS was capable of defining the scope of authorized access of visitors, members and/or users to the website.[22]

B. Contravention of the Void-for-Vagueness Doctrine

1. Applicable Law

Justice Holmes observed that, as to criminal statutes, there is a "fair warning"

---

[22] MySpace utilizes what have become known as "browsewrap" and "clickwrap" agreements in regards to its terms of service. Browsewraps can take various forms but basically the website will contain a notice that - by merely using the services of, obtaining information from, or initiating applications within the website - the user is agreeing to and is bound by the site's terms of service. See Burcham v. Expedia, Inc., 2009 U.S. Dist. LEXIS 17104 at *9-10 n.5 (E.D. Mo. 2009); BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *13-15; Ticketmaster Corp. v. Tickets.Com, Inc., 2003 U.S. Dist. LEXIS 6483 at * 9 (C.D. Cal. 2003) ("[A] contract can be formed by proceeding into the interior web pages after knowledge (or, in some cases presumptive knowledge) of the conditions accepted when doing so."); Specht v. Netscape Communications Corp., 150 F.Supp.2d 585, 594 (S.D.N.Y. 2001), aff'd, 306 F.3d 17 (2d Cir. 2002); Pollstar v. Gigmania, Ltd., 170 F.Supp.2d 974, 981 (E.D. Cal. 2000). "Courts considering browsewrap agreements have held that 'the validity of a browsewrap license turns on whether a website user has actual or constructive knowledge of a site's terms and conditions prior to using the site.'" Burcham, 2009 U.S. Dist. LEXIS 17104 at *9-10 n.5, quoting BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *15-16.

Clickwrap agreements require a user to affirmatively click a box on the website acknowledging awareness of and agreement to the terms of service before he or she is allowed to proceed with further utilization of the website. See Specht, 306 F.3d at 22 n.4; CoStar Realty Info., Inc. v. Field, 612 F.Supp.2d 660, 669 (D. Md. 2009). Clickwrap agreements "have been routinely upheld by circuit and district courts." Burcham, 2009 U.S. Dist. LEXIS 17104 at *8; see also Specht, 306 F.3d at 22 n.4; CoStar Realty Info., 612 F.Supp.2d at 669; DeJohn v. The .TV Corp. Int'l, 245 F.Supp.2d 913, 921 (N.D. Ill. 2003).

As a "visitor" to the MySpace website and being initially limited to the public areas of the site, one is bound by MySpace's browsewrap agreement. If one wishes further access into the site for purposes of creating a profile and contacting MySpace members (as Drew and the co-conspirators did), one would have to affirmatively acknowledge and assent to the terms of service by checking the designated box, thereby triggering the clickwrap agreement. As stated in the MSTOS, "This Agreement is accepted upon your use of the Website or any of the Services and is further affirmed by you becoming a Member." Exhibit 3 at 7; see generally, Doe v. MySpace, Inc., 474 F.Supp.2d 843, 846 (W.D. Tex. 2007).

requirement. As he stated in McBoyle v. United States, 283 U.S. 25, 27 (1931):

> Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear.

As further elaborated by the Supreme Court in United States v. Lanier, 520 U.S. 259, 266 (1997):

> There are three related manifestations of the fair warning requirement. First, the vagueness doctrine bars enforcement of "a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application." Connally v. General Constr. Co., 269 U.S. 385, 391 (1926) . . . . Second, as a sort of "junior version of the vagueness doctrine," H. Packer, The Limits of the Criminal Sanction 95 (1968), the canon of strict construction of criminal statutes, or rule of lenity, ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered . . . . Third, although clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute, . . . due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope. . . . In each of these guises, the touchstone is whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal. [Citations omitted.]

The void-for-vagueness doctrine has two prongs: 1) a definitional/notice sufficiency requirement and, more importantly, 2) a guideline setting element to govern law enforcement. In Kolender v. Lawson, 461 U.S. 352, 357-58 (1983), the Court explained that:

> As generally stated, the void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforce-ment . . . . Although the doctrine focuses both on actual notice to citizens and arbitrary enforcement, we have recognized recently that the more important aspect of the vagueness doctrine "is not actual notice, but the other principal element of the doctrine – the requirement that a legislature establish minimal guidelines to govern law enforcement."

> Smith [v. Goguen], 415 U.S. [566,] 574 [1974]. Where the legislature fails to provide such minimal guidelines, a criminal statute may permit "a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections." Id. at 575. [Footnote and citations omitted.]

To avoid contraving the void-for-vagueness doctrine, the criminal statute must contain "relatively clear guidelines as to prohibited conduct" and provide "objective criteria" to evaluate whether a crime has been committed. Gonzalez v. Carhart, 550 U.S. 124, 149 (2007) (quoting Posters 'N' Things, Ltd. v. United States, 511 U.S. 513, 525-26 (1994)). As stated in Connally v. General Construction Co., 269 U.S. 385, 391-92 (1926):

> The question whether given legislative enactments have been thus wanting in certainty has frequently been before this court. In some of the cases the statutes involved were upheld; in others, declared invalid. The precise point of differentiation in some instances is not easy of statement. But it will be enough for present purposes to say generally that the decisions of the court upholding statutes as sufficiently certain, rested upon the conclusion that they employed words or phrases having a technical or other special meaning, well enough known to enable those within their reach to correctly apply them, . . . or a well-settled common law meaning, notwithstanding an element of degree in the definition as to which estimates might differ, . . . or, as broadly stated . . . in United States v. Cohen Grocery Co., 255 U.S. 81, 92, "that, for reasons found to result either from the text of the statutes involved or the subjects with which they dealt, a standard of some sort was afforded." [Citations omitted.]

However, a "difficulty in determining whether certain marginal offenses are within the meaning of the language under attack as vague does not automatically render a statute unconstitutional for indefiniteness . . . . Impossible standards of specificity are not required." Jordan v. De George, 341 U.S. 223, 231 (1951) (citation and footnote omitted). "What renders a statute vague is not the possibility that it will sometimes be difficult to determine whether the incriminating fact it establishes has been proved; but rather the indeterminacy of precisely what that fact is." United States v. Williams, ___ U.S. ___, 128 S.Ct. 1830, 1846 (2008). In this regard, the Supreme Court "has made clear that scienter requirements alleviate vagueness concerns." Gonzales, 550

U.S. at 149; see also Colautti v. Franklin, 439 U.S. 379, 395 (1979) ("This Court has long recognized that the constitutionality of a vague statutory standard is closely related to whether that standard incorporates a requirement of *mens rea*").

"It is well established that vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in the light of the facts of the case at hand." United States v. Mazurie, 419 U.S. 544, 550 (1975); United States v. Purdy, 264 F.3d 809, 811 (9th Cir. 2001). "Whether a statute is . . . unconstitutionally vague is a question of law . . . ." United States v. Ninety-Five Firearms, 28 F.3d 940, 941 (9th Cir. 1994).

2. Definitional/Actual Notice Deficiencies

The pivotal issue herein is whether basing a CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine. This Court concludes that it does primarily because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies.

As discussed in Section IV(A) above, terms of service which are incorporated into a browsewrap or clickwrap agreement can, like any other type of contract, define the limits of authorized access as to a website and its concomitant computer/server(s). However, the question is whether individuals of "common intelligence" are on notice that a breach of a terms of service contract can become a crime under the CFAA. Arguably, they are not.

First, an initial inquiry is whether the statute, as it is written, provides sufficient notice. Here, the language of section 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that the CFAA has "criminalized breaches of contract" in the context of website terms of service. Normally, breaches of contract are not the subject of criminal prosecution. See generally United States v. Handakes, 286 F.3d 92, 107 (2d Cir. 2002), overruled on other grounds in United States v. Rybicki, 354 F.3d 124, 144 (2d Cir. 2003) (en banc). Thus, while "ordinary people" might expect to be

exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties.[23] Id. This would especially be the case where the services provided by MySpace are in essence offered at no cost to the users and, hence, there is no specter of the users "defrauding" MySpace in any monetary sense.[24]

Second, if a website's terms of service controls what is "authorized" and what is "exceeding authorization" - which in turn governs whether an individual's accessing information or services on the website is criminal or not, section 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will. For example, in the present case, MySpace's terms of service prohibits a member from engaging in a multitude of activities on the website, including such conduct as "criminal or tortious activity," "gambling," "advertising to . . . any Member to buy or sell any products," "transmit[ting] any chain letters," "covering or obscuring the banner advertisements on your personal profile page," "disclosing your password to any third party," etc. See Exhibit 3 at 5. The MSTOS does not specify which precise terms of service, when breached, will result in a termination of MySpace's authorization for the visitor/member to access the website. If any violation of any term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-

---

[23] But see United States v. Sorich, 427 F.Supp.2d 820, 834 (N.D. Ill. 2006), aff'd, 531 F.3d 501 (7th Cir. 2008), cert. denied, 129 S.Ct. 1308 (2009) ("[S]imply because . . . actions can be considered violations of the 'contract' . . . does not mean that those same actions do not qualify as violations of [a criminal] statute.").

[24] Also, it is noted here that virtually all of the decisions which have found a breach of a website's terms of service to be a sufficient basis to establish a section 1030(a)(2)(C) violation have been in civil actions, not criminal cases.

for-vagueness doctrine as to setting guidelines to govern law enforcement.[25]

Third, by utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime, that approach makes the website owner - in essence - the party who ultimately defines the criminal conduct. This will lead to further vagueness problems. The owner's description of a term of service might itself be so vague as to make the visitor or member reasonably unsure of what the term of service covers. For example, the MSTOS prohibits members from posting in "band and filmmaker profiles . . . sexually suggestive imagery or any other unfair . . . [c]ontent intended to draw traffic to the profile." Exhibit 3 at 4. It is unclear what "sexually suggestive imagery" and "unfair content"[26] mean. Moreover, website owners can establish terms where either the scope or the application of the provision are to be decided by them *ad hoc* and/or pursuant to undelineated standards. For example, the MSTOS provides that what constitutes "prohibited content" on the website is determined "in the sole discretion of MySpace.com . . . ." Id. Additionally, terms of service may allow the website owner to unilaterally amend and/or add to the terms with minimal notice to users. See, e.g., id. at 1.

Fourth, because terms of service are essentially a contractual means for setting the scope of authorized access, a level of indefiniteness arises from the necessary application of contract law in general and/or other contractual requirements within the applicable terms of service to any criminal prosecution. For example, the MSTOS has a provision wherein "any dispute" between MySpace and a visitor/member/user arising out of the terms of service is subject to arbitration upon the demand of either party. Before a breach of a term of service can be found and/or the effect of that breach upon MySpace's ability to terminate the visitor/member/user's access to the

---

[25] Another uncertainty is whether, once a user breaches a term of service, is every subsequent accessing of the website by him or her without authorization or in excess of authorization.

[26] See Time Warner Entm't Co., L.P. v. FCC, 240 F.3d 1126, 1135 (D.C. Cir. 2001) ("The word 'unfair' is of course extremely vague.").

site can be determined, the issue would be subject to arbitration.[27] Thus, a question arises as to whether a finding of unauthorized access or in excess of authorized access can be made without arbitration.

Furthermore, under California law,[28] a material breach of the MSTOS by a user/member does not automatically discharge the contract, but merely "excuses the injured party's performance, and gives him or her the election of certain remedies." 1 Witkin, Summary of California Law (Tenth Ed.): Contracts § 853 at 940 (2008). Those remedies include rescission and restitution, damages, specific performance, injunction, declaratory relief, etc. Id. The contract can also specify particular remedies and consequences in the event of a breach which are in addition to or a substitution for those otherwise afforded by law. Id. at § 855 at 942. The MSTOS does provide that: "MySpace.com reserves the right, in its sole discretion . . . to restrict, suspend, or terminate your access to all or part of the services at any time, for any or no reason, with or without prior notice, and without liability." Exhibit 3 at 2. However, there is no provision which expressly states that a breach of the MSTOS automatically results in the termination of authorization to access the website. Indeed, the MSTOS cryptically states: "you are only authorized to use the Services . . . if you agree to abide by all applicable laws and to this Agreement." Id. at 1 (emphasis

---

[27] An arbitration clause is considered to be "broad" when it contains language to the effect that arbitration is required for "any" claim or dispute which "arises out of" the agreement. Fleet Tire Service v. Oliver Rubber Co., 118 F.3d 619, 621 (8th Cir. 1997); see also Schoenduve Corp. v. Lucent Technologies, Inc., 442 F.3d 727, 729 (9th Cir. 2006). Where a broad arbitration clause is in effect, "even the question of whether the controversy relates to the agreement containing the clause is subject to arbitration." Fleet Tire Service, 118 F.3d at 621. Moreover, "[a]n agreement to arbitrate 'any dispute' without strong limiting or excepting language immediately following it logically includes not only the dispute, but the consequences naturally flowing from it . . . ." Management & Tech. Consultants v. Parsons-Jurden, 820 F.2d 1531, 1534-35 (9th Cir. 1987). Further, where the parties have agreed that an issue is to be resolved by way of arbitration, the matter must be decided by the arbitrator, and "a court is not to rule on the potential merits of the underlying claim[] . . . . indeed even if it appears to the court to be frivolous . . . ." AT&T Technologies, Inc. v. Communications Workers of Am., 475 U.S. 643, 649-50 (1986).

[28] According to the MSTOS, "If there is any dispute about or involving the Services, you agree that the dispute shall be governed by the laws of the State of California without regard to conflict of law provisions . . . ." Exhibit 3 at 7.

added).

3. The Absence of Minimal Guidelines to Govern Law Enforcement

Treating a violation of a website's terms of service, without more, to be sufficient to constitute "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" would result in transforming section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals. As noted in Section IV(A) above, utilizing a computer to contact an Internet website by itself will automatically satisfy all remaining elements of the misdemeanor crime in 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A). Where the website's terms of use only authorizes utilization of its services/applications upon agreement to abide by those terms (as, for example, the MSTOS does herein), any violation of any such provision can serve as a basis for finding access unauthorized and/or in excess of authorization.

One need only look to the MSTOS terms of service to see the expansive and elaborate scope of such provisions whose breach engenders the potential for criminal prosecution. Obvious examples of such breadth would include: 1) the lonely-heart who submits intentionally inaccurate data about his or her age, height and/or physical appearance, which contravenes the MSTOS prohibition against providing "information that you know is false or misleading"; 2) the student who posts candid photographs of classmates without their permission, which breaches the MSTOS provision covering "a photograph of another person that you have posted without that person's consent"; and/or 3) the exasperated parent who sends out a group message to neighborhood friends entreating them to purchase his or her daughter's girl scout cookies, which transgresses the MSTOS rule against "advertising to, or solicitation of, any Member to buy or sell any products or services through the Services." See Exhibit 3 at 4. However, one need not consider hypotheticals to demonstrate the problem. In this case, Megan (who was then 13 years old) had her own profile on MySpace, which was in clear violation of the MSTOS which requires that users be

"14 years of age or older." Id. at 2. No one would seriously suggest that Megan's conduct was criminal or should be subject to criminal prosecution.

Given the incredibly broad sweep of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A), should conscious violations of a website's terms of service be deemed sufficient by themselves to constitute accessing without authorization or exceeding authorized access, the question arises as to whether Congress has "establish[ed] minimal guidelines to govern law enforcement." Kolender, 461 U.S. at 358; see also City of Chicago v. Morales, 527 U.S. 41, 60 (1999). Section 1030(a)(2)(C) does not set forth "clear guidelines" or "objective criteria" as to the prohibited conduct in the Internet/website or similar contexts. See generally Posters 'N' Things, Ltd., 511 U.S. at 525-26. For instance, section 1030(a)(2)(C) is not limited to instances where the website owner contacts law enforcement to complain about an individual's unauthorized access or exceeding permitted access on the site.[29] Nor is there any requirement that there be any actual loss or damage suffered by the website or that there be a violation of privacy interests.

The Government argues that section 1030(a)(2)(C) has a scienter requirement which dispels any definitional vagueness and/or dearth of guidelines, citing to United States v. Sablan, 92 F.3d 865 (9th Cir. 1996). The Court in Sablan did observe that:

> [T]he computer fraud statute does not criminalize otherwise innocent conduct. Under the statute, the Government must prove that the defendant intentionally accessed a federal interest computer without authorization. Thus, Sablan must have had a wrongful intent in accessing the computer in order to be convicted under the statute. This case does not present the prospect of a defendant being convicted without any wrongful intent as was the situation in [United States v.] X-Citement Video [513 U.S. 64, 71-73 (1994)].

Id. at 869. However, Sablan is easily distinguishable from the present case as it: 1)

[29] Here, the prosecution was not initiated based on a complaint or notification from MySpace to law enforcement officials.

did not involve the defendant's accessing an Internet website;[30] 2) did not consider the void-for-vagueness doctrine but rather the *mens rea* requirement; and 3) dealt with a different CFAA subsection (i.e. 18 U.S.C. § 1030(a)(5)) and in a felony situation.

The only scienter element in section 1030(a)(2)(C) is the requirement that the person must "intentionally" access a computer without authorization or "intentionally" exceed authorized access. It has been observed that the term "intentionally" itself can be vague in a particular statutory context. See, e.g., American Civil Liberties Union v. Gonzales, 478 F.Supp.2d 775, 816-17 (E.D. Pa. 2007), aff'd, 534 F.3d 181, 205 (3rd Cir. 2008), cert. denied, 129 S.Ct. 1032 (2009).

Here, the Government's position is that the "intentional" requirement is met simply by a conscious violation of a website's terms of service. The problem with that view is that it basically eliminates any limiting and/or guiding effect of the scienter element. It is unclear that every intentional breach of a website's terms of service would be or should be held to be equivalent to an intent to access the site without authorization or in excess of authorization. This is especially the case with MySpace and similar Internet venues which are publically available for access and use. See generally BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *43. However, if every such breach does qualify, then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution. All manner of situations will be covered from the more serious (e.g. posting child pornography) to the more trivial (e.g. posting a picture of friends without their permission). All can be prosecuted. Given the "standardless sweep" that results, federal law enforcement

[30] In Sablan, the defendant was a bank employee who had been recently fired for circumventing its security procedures in retrieving files. Early one morning, she entered the closed bank through an unlocked door and, using an unreturned key, went to her former work site. Utilizing an old password, she logged onto the bank's mainframe where she called up several computer files. Although defendant denied any additional actions, the government charged her with changing certain files and deleting others. As a result of her conduct, several bank files were severely damaged. See 92 F.3d at 866.

entities would be improperly free "to pursue their personal predilections."[31] Kolender, 461 U.S. at 358 (citing Smith v. Goguen, 415 U.S. 566, 575 (1994)).

In sum, if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]." City of Chicago, 527 U.S. at 64.

V. CONCLUSION

For the reasons stated above, the Defendant's motion under F.R.Crim.P. 29(c) is GRANTED.

DATED: This 28th day of August, 2009

GEORGE H. WU
United States District Judge

[31] In comparison, the felony violation of 18 U.S.C. § 1030(a)(2)(C) contains effective scienter elements because it not only requires the intentional accessing of a computer without authorization or in excess of authorization, but also the prerequisite that such access must be "in furtherance" of a crime or tortious act which, in turn, will normally contain additional scienter and/or wrongful intent conditions.