Washington Journal of Law, Technology & Arts

Volume 3 | Issue 3 Article 2

2-14-2007

Suing Based on Spyware? Admissibility of Evidence Obtained from Spyware in Violation of Federal and State Wiretap Laws: *O'Brien v. O'Brien* as a Paradigmatic Case

Shan Sivalingam

Litigation
Cite as: Shan Sivalingam, *Suing Based on Spyware? Admissibility of Evidence Obtained from Spyware in Violation of Federal and State Wiretap Laws*, 3 Shidler J. L. Com. & Tech. 9 (Feb. 14, 2007), *at* <http://www.lctjournal.washington.edu/Vol3/a009Sivalingam.html>

SUING BASED ON SPYWARE? ADMISSIBILITY OF EVIDENCE OBTAINED FROM SPYWARE IN VIOLATION OF FEDERAL AND STATE WIRETAP LAWS

O'Brien v. O'Brien as a Paradigmatic Case

Shan Sivalingam[1]

Abstract

Early in 2005, a Florida intermediate appellate court ruled that a trial court adjudicating a divorce proceeding had properly excluded evidence that the wife obtained by installing a spyware program on the husband's computer. The court held that the evidence was an intercepted electronic communication that violated a Florida statute modeled after the Federal Wiretap Act. The Florida court ruled that exclusion fell properly within the discretion of the trial court, despite the fact that the relevant Florida statute did not contain an exclusionary rule for intercepted electronic communications. This Article provides a short overview of the federal and state prohibitions on intercepting electronic communications before examining the Florida court's analysis of how the spyware violated state law. The Article will also examine the scope of the court's holding and whether information obtained from spyware could ever be admissible in court.

Table of Contents

INTRODUCTION

<1>Early in 2005, the Florida District Court of Appeal (Fifth District) issued its ruling in *O'Brien v. O'Brien*.[2] The court affirmed a divorce court's exclusion of evidence that the wife obtained through the use of spyware that she had installed on her husband's computer.[3] The court found that the wife had illegally intercepted electronic communications in violation of Florida's Security of Communications Act (hereinafter "SOCA").[4] The court based its decision on two factors: (1) the Florida Legislature had modeled SOCA after provisions in the Federal Wiretap Act and (2) federal precedent interpreting the federal statute supported a finding of "interception."[5] The court excluded the evidence on the ground that the statutory violation justified the trial judge's exercise of discretion to exclude the evidence.[6]

<2>The court's holding does not explicitly create a blanket exclusionary rule for illegally intercepted electronic communications, but it is susceptible to such an interpretation. Traditionally, courts have held that illegally obtained communications are inadmissible as evidence. However, these holdings pre-date the federal and state statutory prohibitions on interception of electronic communications; courts could not have anticipated the current ubiquitous use of electronic means of communication. Moreover, spyware may provide access to information that cannot be obtained by other means. Because these considerations require a complicated cost/benefit analysis that is within the proper function of Congress and the state legislatures, courts may need to take a case-by-case approach in evaluating whether equity supports admission or exclusion of such evidence.

FEDERAL AND STATE STATUTES PROHIBITING INTERCEPTION OF ELECTRONIC COMMUNICATIONS

<3>Federal statutes have made it illegal to intercept wire and oral communications.[7] With the proliferation of electronic technology, the old framework for making these interceptions required updating. In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA"), thereby amending the

Federal Wiretap Act. As amended by ECPA, the Federal Wiretap Act (or the "Wiretap Act") imposes criminal liability on a person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[9] Forty-nine states and the District of Columbia have their own wiretap statutes — many with language virtually identical to the federal statute.[10] As discussed below, the Federal Wiretap Act and the parallel state anti-interception statutes do not require the exclusion from evidence of intercepted electronic communications.[11]

OVERVIEW OF SPYWARE

i. What is Spyware?

<4> The definition of spyware changes as fast as programmers can develop new software. Generally, spyware is software installed on a computer in order to monitor the target user's computer activity without their knowledge.[12] Spyware usually targets e-mail and chat room activity. However, spyware can record everything the user does on the computer, including financial record keeping, the preparation of documents in a word-processing program, or the updating of business records.[13] Some spyware programs are used to gather personal identifying information such as passwords, credit card numbers, and Social Security numbers, usually for purposes of fraud and identity theft.[14]

<5> Many spyware programs act like cameras, taking a picture of whatever is on the screen every few seconds.[15] These programs may send log files of the activity to an e-mail address where the spy can play back the sessions.[16] Another significant type of spyware captures keystrokes from the target computer, enabling the spy to discover passwords and other confidential information of the target user.

<6>Spyware is most commonly used in a situation where the spy and the target have no prior relationship. A typical scenario involves the computer user being asked to click "yes" or "no" to some prompt in an Internet pop-up window, where either choice results in the installation of spyware on the user's computer.[17] Or spyware may be surreptitiously installed along with a program that the user intentionally downloads off of the Internet.[18] Spyware is used to track information — either for marketing purposes or for more illicit purposes such as identity theft.[19]

ii. Direct Legislative Prohibitions on Spyware

<7> As of September 2006, there is no federal anti-spyware law. Different pieces of anti-spyware legislation have passed the House of Representatives but have not proceeded any further. At the state level, as of September 2006, at least fifteen state legislatures have adopted some form of anti-spyware legislation and at least eighteen states are considering anti-spyware legislation this year.[20] In addition, some states have computer trespass and or computer privacy statutes that effectively prohibit the use of spyware.[21] Thus, spyware users already risk incurring civil or criminal liability in a growing number of states. Practitioners should be aware of the existence of spyware legislation in their jurisdictions regardless of how ECPA impacts the use of spyware.

FACTS OF O'BRIEN

<8> *O'Brien v. O'Brien* began as a divorce action in a Florida county circuit court.[22] During the course of the divorce proceedings, the wife secretly installed a spyware program called Spector on the husband's computer.[23] The spyware program secretly took "snapshots" of what appeared on the computer screen.[24] The frequency of these screen shots allowed the spyware to record online chats, instant messages, incoming and outgoing e-mail messages, and websites visited by the husband.[25] The spyware program apparently captured private online chats between the husband and another woman.[26]

<9>When the husband discovered the spyware, he uninstalled the software program and moved for temporary and permanent injunctions preventing the wife from disclosing the intercepted communications and engaging in similar action in the future.[27] The court granted these motions and the husband's motion to exclude the intercepted communications from evidence.[28] The wife appealed this ruling to the Florida District Court of Appeal.[29]

THE COURT'S REASONING

<10>The trial court found that the wife illegally obtained the evidence through use of a spyware program because it violated the state's statute that prohibits interception and disclosure of wire, oral, or electronic communications.[30] SOCA imposes criminal liability for 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."[31]

<11>The principal issue facing the appellate court was whether or not the use of the spyware constituted "interception" of electronic communications within the meaning of SOCA.[32] By its terms, SOCA seems to apply only to the act of capturing communications while the communications are in transit as opposed to when the communications have already been transmitted. At the outset, the court noted that, "there is a rather fine distinction between what is transmitted as an electronic communication subject to interception and the storage of what has been previously communicated."[33] In drawing this distinction — a question of first impression — the Florida court looked to federal precedent, as the Florida legislature modeled SOCA after a similar provision in the Federal Wiretap Act.[34]

<12>The federal courts have consistently required that electronic communications be acquired contemporaneously with transmission in order to be intercepted within the meaning of the federal statute.[35] The District Court of Appeal held that the Spector spyware program did contemporaneously intercept the husband's electronic communications. The court reasoned that the spyware copied the communication during transmission and routed the copy to a storage file on the computer. The court distinguished this from simply breaking into a computer and retrieving information already stored on the hard drive.[36] Without this distinction, it would be virtually impossible to violate the Federal Wiretap Act (and, by analogy, SOCA) by intercepting e-mail.[37] Furthermore, the appellate court did not believe that the "evanescent time period, where the text image has just become visible on the screen and the communication is no longer in transit, was sufficient to transform a contemporaneous interception into a retrieval from electronic storage.[38]

<13>The court's inquiry did not end with the determination that SOCA had been violated. Neither SOCA nor the federal statute has an exclusionary rule for electronic communications.[39] Thus, the District Court of Appeal still had to determine whether the exclusion of the evidence was proper.[40] In interpreting the federal statute, the federal courts have held that Congress intended that electronic communications not be excluded under the Federal Wiretap Act.[41] The appellate court's decision turned on the fact that the trial court's ruling to admit or exclude evidence was subject to a deferential abuse of discretion standard.[42] Because the evidence was obtained in violation of SOCA, the trial court was within its discretion in refusing to

admit the evidence.[43]

POTENTIAL IMPACT OF THE COURT'S DECISION

i. Factual Distinctions of O'Brien

<14>The court's holding in *O'Brien* begs the question of whether evidence obtained via spyware may ever be admissible in court. It is useful to scrutinize and vary the facts of the case to determine the limits of liability resulting from the operation of spyware. The circumstances of *O'Brien* suggest that another court may limit the holding to its facts. Here, a wife deliberately installed spyware on her husband's computer, possibly with the intent of proving his infidelity.[44] It is also possible that the wife was trying to discover the true nature of the husband's financial situation in order to obtain a more favorable divorce settlement. In either case, the wife installed the spyware with the intention of using the information obtained as evidence against the husband in a divorce proceeding. However, categorical exclusion of all evidence obtained from spyware would have extremely broad reach, and such a rule would extend beyond the facts of *O'Brien*.

<15>The court in *O'Brien* made reference to the "[h]usband's computer,"[45] but an interesting question is whether the wife would have violated SOCA if the computer had been shared by the two. The wife might then have argued that she could not have violated the statute by installing spyware on her own property (or shared property). Such an argument would face at least two obstacles. First, as mentioned above, some states have computer privacy and computer trespass statutes that preclude spyware users from spying on a spouse's or partner's computer activity, regardless of computer ownership.[46] Second, and more importantly, the prohibition in the Wiretap Act (and in SOCA, as well) against interception of electronic communications applies to any person who is not "party to the communication" where no party to the communication has given consent to the interception.[47] Thus, regardless of computer ownership, both the federal statute and the Florida statute are violated when no party to the communication has consented to the interception.

<16>Another scenario in which spyware may be employed is in the context of an employer-employee relationship. A business may wish to use spyware on employee computers to ensure that employees are not divulging trade secrets and intellectual property, or to prevent, minimize, or deter involvement in online pornography and gambling. Traditionally, employers have had

broad authority to know how their own computers are being used and, thus, employee privacy in work-place computers has been subject to limitations.[48] In special circumstances, courts have gone so far as to allow a digital image to be made of an employee's *personal* computer where there is evidence that the employee has divulged a company's trade secrets.[49] But independent of an individual employee's expectation of privacy, the Wiretap Act's prohibition against interception of electronic communications applies to persons who are not "party to the [intercepted] communication."[50]

ii. Legal Rationale for Not Adopting a Blanket Exclusionary Rule

<17> The holding in *O'Brien*, excluding evidence of an intercepted electronic communication from a civil divorce proceeding, must be viewed in that context when considering its precedential value.[51] Whether or not an intercepted electronic communication may be introduced as evidence, absent a statutory exclusionary rule, is a relatively new legal issue. When prohibited by statute, courts have focused on whether an illegal interception of electronic communications has taken place at all.[52] Given the novelty of the issue decided in *O'Brien*, it is useful to look to case law on the exclusion of other intercepted communications in order to understand the courts' approach to dealing with illegally-obtained evidence. It is also essential to note that exclusion of evidence in a civil proceeding differs in important ways from excluding evidence in a criminal proceeding.

<18> Generally, courts have held that evidence obtained through illegal interception of communications is inadmissible. The United States Supreme Court has held that communications intercepted in violation of federal law may not be introduced in a state court.[53] Most state courts have also held that evidence obtained by illegally intercepting communications may not be admitted in evidence.[54] However, these decisions generally deal with interception of wire or oral communications and were also decided before Congress enacted ECPA in 1986.[55] Moreover, the cited decisions all arose from criminal prosecutions. In contrast to civil lawsuits, where a losing defendant faces pecuniary loss, a criminal defendant attempting to suppress illegally-intercepted evidence may be facing imprisonment. The age of these cases, their criminal context, and the fact that ECPA omits an exclusionary rule for intercepted electronic communications counsel against a judge-made blanket exclusionary rule for illegally-intercepted electronic communications.

<19>Also, the illegal wiretapping at issue in *O'Brien* was conducted by an individual in a civil proceeding, not by the state. Because the Fourth Amendment is not implicated in the absence of state action, O'Brien's conduct was illegal only to the extent that it violated a statute or the common law tort of privacy.[56] For statutory and common law violations, especially where the statute intentionally omits a rule of exclusion, the need for a universal exclusionary rule is not as obvious.[57] One can imagine a scenario in which electronic communications intercepted by spyware in violation of ECPA might be held admissible. Such a scenario would likely arise in the workplace context, where, as stated above, employers have broad authority to search their employees' computers.[58] If a company sued its employee for divulging trade secrets, the rationale for excluding evidence of the misconduct, obtained from spyware, is not as compelling as the Florida court's rationale in *O'Brien*.

iii. Impact of United States v. Councilman

<20>When considering the potential impact of *O'Brien* with regard to ECPA and its state law analogs, practitioners will look to the most recent case from a federal appeals court analyzing interception of electronic communications, *United States v. Councilman*.[59] Bradford Councilman was a principal officer of Interloc, Inc., an online rare and out-of-print book listing service.[60] As part of its service, Interloc gave book dealer customers an e-mail address at the domain "interloc.com" and acted as the e-mail provider.[61] At Councilman's direction, Interloc employees intercepted and copied all incoming communications to subscriber dealers from Amazon.com — a competitor of Interloc — with the hope of gaining a competitive edge.[62] Interloc's e-mail system was modified so that, before delivering any message from Amazon.com to the recipient's @interloc.com mailbox, the message would be copied and placed in a separate mailbox that Councilman had access to.[63] This intercept occurred during the e-mail transmission process, but while each message was in a state of temporary storage.

<21>The United States Court of Appeals for the First Circuit, sitting en banc, reversed the district court's decision and held that Councilman's actions did violate the Wiretap Act.[64] Prior to *Councilman*, courts had held that violation of the Wiretap Act could not occur without interception that occurs contemporaneous with transmission.[65] The First Circuit in *Councilman* held that the term "electronic communication" in the ECPA statute includes transient electronic storage that is intrinsic

to the communication process.[66] Thus, interception of an e-mail message in such transient storage violated ECPA.[67]

<22>The First Circuit's holding in *Councilman* does not conflict with the Florida court's decision in *O'Brien*. In *O'Brien*, the wife could have argued that the interception of data occurred while her husband's e-mail messages and chats were in storage. However, such storage would be just as transitory as the storage involved in *Councilman*. In either case, a party's actions violated a prohibition against the interception of electronic communications.

<23>*Councilman*, however, involved a criminal prosecution and the evidence obtained in violation of the Wiretap Act was introduced by the government. It is interesting to note that the government may use information obtained by a criminal defendant in violation of ECPA to the defendant's detriment (to prove that Councilman was conspiring to gain an advantage over Amazon.com). *Councilman* thus serves as a potential warning that the use of spyware could be a double-edged sword. Evidence obtained from spyware will be inadmissible as against the targeted party, but the government may use evidence obtained from spyware in a criminal prosecution of the spyware user.

CONCLUSION

<24> The extent to which evidence obtained from spyware shall be admissible in court requires determinations of values that are traditionally left in the hands of the legislative branch of government. Here, however, Congress and the state legislatures seem to have made a conscious decision against exclusion of evidence derived from an illegal electronic interception, since exclusion of evidence derived from illegal wire and oral interceptions is mandatory. Under these circumstances a blanket exclusionary rule is not warranted. Unless the legislative branch affirmatively acts, exclusion of evidence obtained through spyware may best be left to the sound discretion of the trial court — as was the case in *O'Brien*.

PRACTICE POINTERS

- Never counsel a client to take action that could violate the Federal Wiretap Act or a state law analog. Although exclusion of evidence obtained in violation of the federal statute is not required, courts have broad discretion in admitting and excluding

evidence. An appellate court may be hesitant to overrule a trial court's decision to exclude evidence that was obtained in violation of a criminal statute.

- Advise organizational clients to develop and implement computer usage policies that grant the employer broad authority to monitor employee computers to minimize the information security threat that spyware poses. Ensure that employees agree to abide by such policies as a condition of employment.

<< Top

Footnotes

1. Shan Sivalingam, University of Washington School of Law, Class of 2007. Thank you to my peers on the Shidler Journal editorial staff, Professor Anita Ramasastry of the University of Washington School of Law, and to Floyd G. Short of Susman Godfrey L.L.P. for their invaluable contributions to this Article.

2. O'Brien v. O'Brien, 899 So. 2d 1133 (Fla. Dist. Ct. App. 2005), reh'g denied (Fla. 2005).

3. *Id.* at 1134.

4. FLA. STAT. §§ 934.01-934.07 (2003). In pertinent part, the Florida statute imposes criminal liability on any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." § 934.03(1)(a). The Security of Communication Act should not be confused with the Federal Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2711 (2000).

5. 18 U.S.C. § 2511 (2000). The Florida statute was modeled after the Federal Electronic Communications Privacy Act ("ECPA") — a 1986 amendment to the Federal Wiretap Act.

6. Note: This Article focuses on the federal and state prohibitions against interception of electronic communications as a bar to the admissibility of information obtained from spyware. The Article does not reach other statutory and evidentiary grounds for excluding such evidence.

7. 18 U.S.C. § 2510 (2000).
8. 18 U.S.C. § 2511.
9. 18 U.S.C. § 2511(1)(a).
10. National Conference of State Legislatures (2006), http://www.ncsl.org/programs/lis/CIP/surveillance.htm (last visited February 1, 2007). *See, e.g.*, HAW. REV. STAT. § 803-42 (2005).
11. *See* 18 U.S.C. § 2515 (2000).
12. Sharon D. Nelson & John W. Simek, *Muddy Waters: Spyware's Legal and Ethical Implications*, GPSOLO MAGAZINE, ABA General Practice, Solo & Small Firm Division (Jan./Feb. 2006).
13. *Id.*
14. *Id.*
15. *Id.*
16. *Id.*
17. *See, e.g.*, Sarah Gordon, *Elusive Intruders: Spyware & Adware*, 22 No. 16 LAW. PC 8 (May 15, 2005).
18. *See, e.g.*, Jane K. Winn, *Contracting Spyware by Contract*, 20 BERKELEY TECH. L.J. 1345, 1347-48 (Summer 2005).
19. *Id.* at 1347.
20. The following states have adopted anti-spyware legislation: Alaska, Arizona, Arkansas, California, Georgia, Indiana, Iowa, Hawaii, Louisiana, New Hampshire, Tennessee, Texas, Utah, Virginia, and Washington. National Conference of State Legislatures (2006), http://www.ncsl.org/programs/lis/spyware06.htm (last visited February 1, 2007). *See, e.g.*, WASH. REV. CODE § 19.270.010-.270.900 (2006).
21. *See, e.g.*, VA. CODE ANN. § 18.2-152.5 (2006).
22. O'Brien v. O'Brien, 899 So. 2d 1133, 1134 (Fla. Dist. Ct. App. 2005), reh'g denied (Fla. 2005).
23. *Id.*
24. *Id.*
25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.*

30. FLA. STAT. § 934.03 (2003).

31. FLA. STAT. § 934.02(3) (defining the term "intercept").

32. *O'Brien*, 899 So. 2d at 1135.

33. *Id.*

34. *Id.* at 1135-36; 18 U.S.C. § 2510, et seq. (2000).

35. 18 U.S.C. § 2511; 899 So. 2d at 1136 (citing Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003); Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir.), *cert. denied*, 160 L. Ed. 2d 17, 125 S. Ct. 48 (2004); United States v. Steiger, 318 F.3d 1039 (11th Cir.), *cert. denied*, 538 U.S. 1051 (2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003)).

36. *O'Brien*, 899 So. 2d at 1136-37 (citing *Steiger*, 318 F.3d at 1050).

37. Violation of the statutes might still be possible if the hacked computer had some type of automatic routing software installed. Jarrod J. White, *E-Mail at Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1083 (1997).

38. *O'Brien*, 899 So. 2d at 1137.

39. *Id.* (citing FLA. STAT. § 934.06 (2003) ("[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication . . . may be received in evidence . . . ")); 18 U.S.C. § 2515.

40. *O'Brien*, 899 So. 2d at 1137.

41. *Id.*; United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003) ("[b]y its terms, 18 U.S.C. § 2515 [ECPA's exclusionary rule] applies *only* to 'wire or oral communications,' and not to 'electronic communication[s]'").

42. *O'Brien*, 899 So. 2d at 1137-38.

43. *Id.*

44. *See id.* at 1134.

45. *Id.* at 1134.

46. *See, e.g.*, N.C. GEN. STAT. § 14-458 (2006) ("[I]t shall be unlawful for any person to use a computer . . . without authority and with the intent to . . . [m]ake . . . an unauthorized copy . . . of computer data . . . ;" "a person is 'without authority' when (i) the person has no right or permission of the owner to use a computer, or the person uses a computer in a manner exceeding the right or permission").

47. *See* 18 U.S.C. § 2511(2)(d) (2000); FLA. STAT. § 934.03(2)(d) (2003).

48. Greenberg v. Alta Healthcare Sys., 2004 WL 859185, at *3 (Cal. App. Apr. 22, 2004) (holding that hospital employee has no expectation of privacy in computer files stored on her hospital computer).

49. Quotient, Inc. v. Toon, 2005 WL 4006493, at *1, 4 (Md. Cir. Ct. Dec. 23, 2005) (allowing employer's forensic computer expert to make a digital image of employee's personal computer hard disk to prevent intentional and unintentional destruction of data).

50. *See* 18 U.S.C. § 2511(2)(d).

51. FLA. STAT. § 934.03; *see also* Mark Gruber, *How to Minimize Your Risk of Being Sued*, 27 FAMILY ADVOCATE 48 (Spring 2005) (advising family law practitioners to "[n]ever use or endeavor to use evidence obtained in violation of wiretap statutes").

52. *See, e.g.*, Hall v. Earthlink, 396 F.3d 500 (2d Cir. 2005) (internet service provider's receipt and storage of a customer's e-mails did not constitute interception of electronic communications within the meaning of the Federal Wiretap Act; court did not reach the question of whether intercepted communications were admissible in evidence).

53. 8 JOHN H. WIGMORE, WIGMORE ON EVIDENCE § 2184b(2) (2005-2 Cumulative Supplement – Arthur Best – Aspen Publishers, New York, NY) (citing Lee v. Florida, 392 U.S. 378 (1968)).

54. *See* WIGMORE, *supra* note 53, at § 2184b(2) (citing Tavernetti v. Superior Court, 22 Cal. 3d 187, 583 P.2d 737 (1978) (evidence obtained by illegal

electronic eavesdropping held inadmissible); People v. Kezerian, 63 Ill. App. 3d 610, 379 N.E.2d 1246 (1978) ("fruit of the poisonous tree" doctrine prevents admission of evidence indirectly obtained as a result of information acquired through violation of state eavesdropping statute)). *But see* People v. Maranian, 359 Mich. 361, 102 N.W.2d 568 (1960) (placing recording device on receiver's telephone did not constitute wiretapping).

55. 18 U.S.C. § 2511 (2000).

56. The Florida court did not explicitly hold that the intercepted communications violated the Federal Wiretap Act – although the analysis logically leads to that conclusion. O'Brien v. O'Brien, 899 So. 2d 1133, 1135-37 (Fla. Dist. Ct. App. 2005), reh'g denied (Fla. 2005).

57. *Id.* at 1137.

58. *See* Quotient, Inc. v. Toon, 2005 WL 4006493, at *1, 4 (Md. Cir. Ct. Dec. 23, 2005).

59. United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc), *rev'g* 373 F.3d 197 (1st Cir. 2004).

60. *Id.* at 70.

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.* at 85.

65. Fresser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003); Konop v. Hawaiian Airlines, 302 F.3d 868, 878 (9th Cir. 2002); Steve Jackson Games, Inc. v. U. S. Secret Serv., 36 F.3d 457 (5th Cir. 1994).

66. *Councilman*, 418 F.3d at 85.

67. *Id.* For a thorough discussion of the impact of *Councilman*, *see* Jessica Belskis, Note, *Applying the Wiretap Act to Online Communications after United States v. Councilman*, 2 SHIDLER J. L. COM. & TECH. 18 (Apr. 14, 2006).

<< Top