Washington Journal of Law, Technology & Arts

Volume 2 | Issue 4 Article 4

4-14-2006

Applying the Wiretap Act to Online Communications after *United States v. Councilman*

Jessica Belskis

Constitutional & Regulatory
Cite as: Jessica Belskis, *Applying the Wiretap Act to Online Communications after* United States v. Councilman, 2 Shidler J. L. Com. & Tech. 18 (Apr. 14, 2006), *at* <http://www.lctjournal.washington.edu/Vol2/a018Belskis.html>

APPLYING THE WIRETAP ACT TO ONLINE COMMUNICATIONS AFTER UNITED STATES V. COUNCILMAN

Jessica Belskis[1]

Abstract

This article examines the federal Wiretap Act and its application to online communications in light of the United States Court of Appeals for the First Circuit's recent decision in *United States v. Councilman*. The federal Wiretap Act places legal limits on the surveillance of electronic communications, but courts struggle to make sense of its application to online communications. Formerly, courts held that the Wiretap Act did not apply to the retrieval of communications from places of electronic storage. However, in *United States v. Councilman*, the First Circuit suggests that retrieval of emails from temporary places of electronic storage fall within the Wiretap Act. In order to avoid liability, businesses that monitor customers online should seek customer consent and familiarize themselves with different interpretations of the federal statute as well as various state wiretap statutes.

Table of Contents

INTRODUCTION

<1> To what extent can businesses legally gather customer

information through computer or online surveillance? Businesses commonly place cookies[2] on customer computers, and some businesses, such as Google with its Gmail service, scan emails to learn customers' buying habits, preferences and personal information. The federal Wiretap Act regulates online and computer surveillance;[3] however, the Act is "a complex, often convoluted, area of the law,"[4] and relatively few cases have interpreted the Act's application to online surveillance. Recently, the United States Court of Appeals for the First Circuit clarified the application of the Act to email communications in *United States v. Councilman*.[5] Businesses should be aware of *Councilman*'s implications when creating online monitoring systems.

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

<2> In 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act, the precursor to the Electronic Communications Privacy Act (ECPA).[6] Title III of the Omnibus Crime Control and Safe Streets Act, known as the Wiretap Act, addressed the interception of wire and oral communications.[7]

<3> In 1986, Congress enacted the ECPA[8] in order to expand the protections of the Wiretap Act. The stated purpose of the ECPA is to "protect against the unauthorized interception of electronic communications … [and] update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[9] The ECPA broadens the scope of the earlier statute by including, most notably, coverage of electronic communications.

<4> The ECPA consists of two titles: the Wiretap Act and the Stored Communications Act. Title I, the Wiretap Act, prohibits anyone from "intentionally intercept[ing] or endeavor[ing] to intercept any wire, oral, or electronic communication."[10] The Wiretap Act exempts wire and electronic communication service providers acting in their normal course of business. The Wiretap Act also exempts situations where one party to the intercepted communication grants consent.[11] Title II, the Stored Communications Act, prohibits anyone from "intentionally access[ing] without authorization a facility through which an electronic communication service is provided" and from "intentionally exceed[ing] an authorization to access that facility."[12] The Stored Communications Act exempts providers of electronic or wire communications services, regardless of whether the provider acts in the normal course of business.[13]

<5> Liability under the Wiretap Act (hereinafter "the Act")

requires three elements. First, the Act requires proof of specific intent.[14] Under this element, a party must intentionally or recklessly disregard the law in order to be found liable.[15]

<6> Second, the Act requires presence of a "wire, oral, or electronic communication."[16] These elements are separately defined by the Act. For example, "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." Therefore, computer communications are electronic communications under the Act.[17] In order to demonstrate the presence of a wire, oral, or electronic communication, a party bringing a suit under the Act must have entertained a reasonable expectation of privacy.[18] Where a party's conversation takes place using loud voices in a small room while in the presence of other persons, and the conversation can be heard with "[a] naked ear under uncontrived circumstances," there can be no reasonable expectation of privacy.[19] In such a case, the party's suit would fail for lack of an oral communication as defined by the Act.

<7> The third element of liability under the Act is "interception."[20] Interception has proven to be the trickiest aspect of the statute, and most debate surrounding the Wiretap Act's application to computer and internet surveillance examines this fuzzy concept. The statute defines "intercept" as 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."[21] The Act defines electronic, mechanical, or other devices as "any device or apparatus which can be used to intercept a wire, oral or electronic communication" other than instruments furnished to the subscriber of a communication service or being used by a provider of a communication service in the ordinary course of its business.[22]

<8> Under the Act, interception refers to third-party acquisition of communication *contents* but not *transactional* information.[23] Transactional information consists of information related to user transactions, such as dialing, routing, addressing, and signaling information. Cookies normally register transactional data and do not intercept content of communications; therefore, the Wiretap Act generally does not cover cookies. *In re DoubleClick Inc. Privacy Litigation* exemplifies this distinction.[24] In *DoubleClick*, a corporate provider of internet advertising products and services

used cookies to collect information about Internet users in order to target online advertising. Plaintiffs argued that the cookies were "wiretaps" intercepting their communications. The United States District Court for the Southern District of New York held, however, that there was no violation of the Wiretap Act. Although the court based its decision on a consent theory, commentators generally refer to this case to articulate the content-transactional distinction.[25] The section below further explores the concept of interception.

<9> The Wiretap Act contains two major exceptions. First, no violation takes place when a communication service provider, whose facilities are used in the transmission of the communication, intercepts a communication in the normal course of business or when the interception is necessary to protect the property or rights of the provider.[26] Second, the statute makes interception permissible where at least one party to the communication gives prior consent.[27]

UNITED STATES V. COUNCILMAN AND THE MEANING OF "INTERCEPTION"

<10> Circuit Courts of Appeal that have considered the matter have traditionally held that "'intercept' under the ECPA must occur contemporaneously with transmission."[28] According to this theory, the Wiretap Act does not cover communications sitting in any type of electronic storage, because interception does not occur instantaneously with transmission. Therefore, where a communication is sent but remains unopened in the recipient's computer, third-party acquisition of this stored communication does not violate the Wiretap Act. For example, where the Secret Service seized a computer used to operate an electronic bulletin board system containing private electronic mail messages which had not yet been retrieved by their intended recipients, the Fifth Circuit Court of Appeals held there was no violation of the Wiretap Act because the definition of "electronic communication" does not include electronic storage of such communications.[29]

<11> The Ninth Circuit Court of Appeals similarly held that a lawyer who used a patently unlawful subpoena to gain access to email stored by an Internet service provider did not violate the Wiretap Act because the "Act only applies to the acquisition contemporaneous with transmission," and "Congress did not intend for 'intercept' to apply to 'electronic communications' when those electronic communications are in electronic storage."[30] In *Konop v. Hawaiian Airlines*, the Ninth Circuit Court of Appeals held that when the vice president of Hawaiian

Airlines accessed the plaintiff pilot's website without permission, there was no violation of the Wiretap Act. The Court found that "[f]or a website such as Konop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."[31] The Eleventh Circuit Court of Appeals ruled that when an individual used a Trojan Horse virus to hack into another's computer and download files stored on the computer's hard drive, there was no violation of the Act[32] because "a contemporaneous interception—i.e., an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications."[33]

<12> What happens when the interception of a communication occurs both: (1) contemporaneously with transmission; and (2) while the communication sits in a location of electronic storage? "Traveling the internet, electronic communications are often—perhaps constantly—both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox."[34] *United States v. Councilman* posed this vexing issue to the First Circuit Court of Appeals.[35] The First Circuit initially ruled that such an acquisition does not violate the Wiretap Act (*Councilman I*).[36] However, the court reversed following an en banc rehearing, holding that such acquisition does constitute an interception and, therefore, violates the Wiretap Act (*Councilman II*).[37]

<13> In *Councilman*, defendant Bradford C. Councilman was the vice-president of an online rare and out-of-print book listing service called Interloc. In addition to the book listing service, Interloc provided customers with email accounts and acted as a service provider for these accounts. In order to better target customers and respond to growing competition from Amazon.com, Interloc intercepted and copied email communications sent from Amazon.com to its customers before delivering the messages into customer email accounts. Plaintiffs charged that Councilman violated the Wiretap Act by intercepting these email communications. The Stored Communications Act was inapplicable in this case due to a statutory exception that exempts communication service providers.[38]

<14> The process of email transmission technically enables an email message to sit in electronic storage during the process of transmission. Email operates by splitting a message into small packets and then transferring these packets from computer to computer until the packets reach their final destination, where they are reconfigured.[39] As packets travel from computer to computer, they are stored in intermediary locations called

Message Transfer Agents (MTA).[40] Each MTA stores the message locally before routing it through to another MTA until the message ultimately reaches the recipient's mail server. Email service providers often use separate Mail Delivery Agents (MDA) to retrieve messages from the MTA and deliver them to recipients. Interloc used a program called procmail as its MDA. Interloc rewrote the procmail program code so that it intercepted, copied, and stored all incoming emails from Amazon.com before delivering them into recipients' email boxes.[41] The procmail program operated while messages were stored in the random access memory (RAM) or hard disks within the Interloc system. Therefore, Interloc intercepted the customer emails from temporary storage within Interloc's own computer system. Councilman argued that because the communications were copied from electronic storage and because the term "electronic communication" does not include "electronic storage," there was no interception as contemplated by the Wiretap Act.[42]

<15> In *Councilman I*, the First Circuit Court of Appeals ruled that Councilman did not violate the Wiretap Act because the email communications at issue were intercepted while in electronic storage. The Wiretap Act defines "wire communication" to include "any electronic storage" of wire communications[43] and defines "electronic storage" as "any temporary, intermediate storage."[44] On the other hand, the Wiretap Act's definition of "electronic communication" contains no mention of electronic storage. The First Circuit found that the inclusion of electronic storage within the statutory definition of wire communication, and the exclusion of electronic storage from the definition of electronic communication, suggests that "Congress did not intend for the Wiretap Act's interception provisions to apply to communication in electronic storage."[45]

<16> The *Councilman I* court acknowledged the problem of contemporaneity and conceded that Interloc intercepted emails contemporaneously as they were being transmitted. [46] However, the court explained that the contemporaneity rule was trumped because of: (1) the exclusion of "electronic storage" from the definition of "electronic communication"; (2) "the presence of the words 'any temporary intermediate storage'" within the definition of "electronic storage"; and (3) the fact that "the electronic communications in this case were in a form of electronic storage."[47] Because procmail performed its operations while the communications were stored in RAM or hard disks within Interloc's computer system, the communications were outside the scope of "electronic

communication."

<17> The *Councilman I* court explained that Congress's omission of "electronic storage" from the definition of "electronic communication" indicated that Congress meant to provide lesser protection to electronic communications than to wire and oral communications. Even if the omission was accidental, "it is not the province of this court to graft meaning onto the statute where Congress has spoken plainly."[49]

<18> In October 2004, a majority of the First Circuit agreed to rehear Councilman en banc,[50] whereupon the court withdrew and vacated the prior judgment. In *Councilman II*, the First Circuit ruled that the "electronic communication" includes "transient electronic storage that is intrinsic to the communication process." Therefore, the court ruled that interception of an email communication in transient electronic storage violates the Wiretap Act.[51]

<19> In *Councilman II*, the court conceded that a plain meaning interpretation of the Wiretap Act suggests that "electronic communication" does not include transient electronic storage. The court explained the Russello maxim as holding that "where Congress includes particular language in one section of the statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."[52] However, the court noted that the Russello maxim holds true only where Congress acted deliberately and carefully in choosing its words of construction and where the provisions' language, structure and circumstances of enactment are analogous.[53] The definitions of "electronic communication" and "wire communication" were constructed at different times and under different circumstances, and contain language that is not parallel. Accordingly, it cannot be inferred that Congress intended to exclude transient stored communications from the definition of "electronic communications."[54]

<20> In order to ascertain the true meaning of "electronic communications," the court looked to legislative intent. House reports and hearings indicated that Congress intended to protect "pre- and post-transmission 'temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission."[55] According to the court, although the statute defines "electronic storage" broadly to include any temporary or intermediate storage, the purpose of this broad definition is to heighten privacy protection for stored data and not to exclude email messages stored during transmission.[56] In addition, by

including "electronic storage" in the definition of "wire communication," Congress intended to ensure the protection of voice mail and did not intend to affect the protection of email.[57]

<21> Although the *Councilman* facts involved interception of email communications contemporaneous with transmission, the First Circuit did not base its decision on the rule of contemporaneity. In dicta, the *Councilman II* court states that it did not address the issue of "whether the term 'intercept' applies only to acquisitions that occur contemporaneously with the transmission of a message from sender to recipient, or, instead, extends to an event that occurs after a message has crossed the finish line of transmission."[58] The opinion says that the traditional rule requiring a real-time interception may not be apt for questions involving the application of the Wiretap Act to electronic communications. In doing so, the First Circuit leaves open the possibility of a more expansive application of the Wiretap Act to post-transmission email communications that have arrived at the destination computer, but sit in storage at the destination unopened.

IMPLICATIONS FOR ONLINE BUSINESSES

<22> Violators of the Wiretap Act can be fined or imprisoned for up to five years.[59] Although only time will tell whether other federal circuits will follow the *Councilman II* holding, online businesses should avoid unreasonable risk. Businesses should presume that *Councilman II*'s stricter rendition of the statute is correct, and they should comply accordingly. Under *Councilman II*, scanning customer emails or placing cookies on customer computers in order to surreptitiously intercept content of communications could result in liability under the Wiretap Act, even if the intercepted data technically sits in "electronic storage" during transmission. Businesses wishing to use these methods to collect customer information should first seek clear consent from customers.

<22> The Wiretap Act's consent exception allows interception of an electronic communication "where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception."[60] Consent can be express or implied, and courts generally look at the overall circumstances when making a determination.[61] In order to be safe, businesses should seek express written consent.

<23> Consent agreements should be broadly written to include

all types of information businesses might collect. After acquiring consent, businesses should stay well within the bounds of their agreement. When a data collection business serving online pharmaceutical companies used cookies to collect customer names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, and medications, the First Circuit held that the data collection business exceeded its consent by collecting such personally identifiable information. The court determined that the customer pharmaceutical companies agreed only to the interception of a subset of these communications.[62] In addition, businesses should enable customers to take simple steps to avoid collection of their personal information. Where an online advertising company used cookies to collect personal user information and create detailed user profiles, the United States District Court for the Southern District of New York determined that the company did not violate the Wiretap Act because it only collected transactional data and enabled users to prevent data collection by visiting a special website and requesting an "opt-out" cookie.[63]

STATE WIRETAP STATUTES

<24> Forty-nine states and the District of Columbia have their own state wiretap statutes.[64] Because states largely modeled their statues after the federal act,[65] and because states cannot "impose requirements less stringent" than the federal standard,[66] state courts often read their wiretap statutes as being consistent with interpretations of the federal act. States may set forth standards stricter than the federal statute.[67] Currently, twelve states have two-party consent requirements, meaning that *both* parties to the communication must give consent in order to make interception of a communication permissible. These states are California,[68] Connecticut,[69] Delaware,[70] Florida, [71] Illinois,[72] Maryland,[73] Massachusetts,[74] Michigan,[75] Montana,[76] New Hampshire,[77] Pennsylvania,[78] and Washington.[79]

<25> Many online businesses appear not to comply with these two-party consent statutes. DoubleClick, for example, has permission from commercial websites to intercept their web communications with their users. However, individual users generally do not consent to the interception of personal information. Google might also be liable under state wiretap statutes for the way it administers its Gmail product.[80] Gmail is an email service provider that provides target advertising to

customers. Advertisers buy keywords from Gmail, and Gmail scans the contents of incoming emails in order to determine which relevant advertisement to display when the recipient opens his or her email. Although Gmail subscribers give consent by signing waivers, individuals who exchange emails with Gmail users do not consent to the interception and scanning of their communications.

<26> Given this appearance of noncompliance, it is somewhat surprising that online businesses have not been summoned to state court for violating two-party consent statutes. Perhaps the traditional rule that a communication must be "contemporaneous with transmission" in order to fall within the Wiretap Statute has deterred nonconsenting parties from filing suit, because this interpretation generally exonerates businesses from liability. *Councilman II* offers a different interpretation so that communications in "electronic storage," which are not necessarily "contemporaneous with transmission," might fall under the purview of the Act. Online businesses should act cautiously and obtain consent from *all* parties to the communication whenever possible.

CONCLUSION

<27> Before implementing customer monitoring or surveillance devices, online businesses should familiarize themselves with both federal and state wiretap statutes. The federal Wiretap Act places legal limits on online and computer surveillance, but courts disagree over application of the Act, making it difficult for online businesses to draw a clear set of guidelines. The First Circuit recently interpreted the Wiretap Act and its application to email in *United States v. Councilman.*[81] Whether other circuits will follow the *Councilman II* interpretation remains unknown; therefore, practitioners and businesses should stay abreast of developments in their jurisdictions.

PRACTICE POINTERS

- Don't intercept content without clear consent. If you wish to intercept the content of a communication, you should first seek express written consent, preferably from *both* parties to the communication.
- Transactional information can be intercepted without consent, but be careful that your transactional interception does not bleed into content interception.
- Write consent agreements broadly to include all

types of information that might be collected. After acquiring consent, you should stay within the bounds of the agreement.

- Consider allowing customers to take simple steps to opt out of collection of personal information.
- Stay tuned for further developments, because other federal Circuit Courts of Appeal may be called upon to adopt or reject the First Circuit's statutory interpretation in *Councilman II*.

<< Top

Footnotes

1. Jessica Belskis, University of Washington School of Law, Class of 2006. Belskis can be reached at jbelskis@u.washington.edu.
2. A cookie is data sent to a computer by a web server that records the user actions on that website. This data generally enables web sites to keep track of user preferences and buying patterns.
3. 18 U.S.C. §§ 2510-2522 (2005).
4. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).
5. United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).
6. Dorothy Higdon Murphy, *United States v. Councilman and the Scope of the Wiretap Act: Do Old Laws Cover New Technologies?* 6 N.C.J.L. & Tech. 437, 441 (Spring 2005).
7. *Id.* at 441.
8. *Id.* at 442 (citing S. Rep. No. 99-541 (1986)).
9. *Id.* at 443 (citing S. Rep. No. 99-541 (1986)).
10. 18 U.S.C. § 2511(1)(a) (2005).
11. 18 U.S.C. § 2511(2) (2005).
12. 18 U.S.C. § 2701(a) (2005).
13. 18 U.S.C. § 2701(c) (2005).
14. 18 U.S.C. § 2511(1)(a) (2005). *See* United States v. Schilleci, 545 F2d 519 (5th Cir. 1977).

15. Citron v. Citron, 539 F. Supp. 621 (S.D.N.Y. 1982), *aff'd*, 722 F.2d 14 (2d Cir. 1983), *cert. denied*, 466 U.S. 973 (1984).

16. 18 U.S.C. § 2511(1)(a) (2005).

17. 18 U.S.C. § 2510(12) (2005).

18. Mitchell Waldman, Annotation, *Expectation of Privacy in Internet Communications*, 92 A.L.R. 5th 15 (2005). *See also* Kemp v. Bock, 607 F. Supp. 1262, 1264-65 (D. Nev. 1985); People v. Suttle, 90 Cal. App. 3d 572, 579 (Cal. Ct. App. 1979).

19. Kemp v. Bock, 607 F. Supp. 1262, 1264-65 (D. Nev. 1985).

20. 18 U.S.C. § 2511(1)(a) (2005).

21. 18 U.S.C. § 2510(4) (2005).

22. 18 U.S.C. § 2510(4) (2005).

23. Orin S. Kerr, *Lifting the Fog of Internet Surveillance: How a Suppression Remedy Would Change Computer Law,* 54 Hastings L.J. 805, 815 (2003).

24. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

25. Kerr, *supra* note 22, at 831.

26. 18 U.S.C. § 2511(2)(a) (2005).

27. 18 U.S.C. § 2511(2)(d) (2005).

28. Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003).

29. Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994).

30. Theofel v. Farey-Jones, 359 F. 3d 1066, 1077 (9th Cir. 2004).

31. Konop v. Hawaiian Airlines, 302 F.3d 868, 878 (9th Cir. 2002).

32. United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003).

33. *Id.* at 1049.

34. U.S. v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003), *aff'd*, 373 F.3d 197 (1st Cir. 2004), *reh'g granted*, 385 F.3d 793 (1st Cir. 2004), *rev'd*,

418 F.3d 67 (1st Cir. 2005) (en banc).

35. U.S. v. Councilman, 373 F.3d 197 (1st Cir. 2004), *aff'g* 245 F. Supp. 2d 319 (D. Mass. 2003), *reh'g granted*, 385 F.3d 793 (1st Cir. 2004), *rev'd*, 418 F.3d 67 (1st Cir. 2005) (en banc).

36. *Id.*

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

38. 18 U.S.C. § 2701(c)(1) (2005).

39. U.S. v. Councilman, 418 F.3d at 69.

40. *Id*.

41. *Id.*

42. *Id.* at 71.

43. 18 U.S.C. § 2510(1) (2005).

44. 18 U.S.C. § 2510(17) (2005).

45. U.S. v. Councilman, 373 F.3d 197, 201 (1st Cir. 2004), *quoting* U.S. v. Councilman, 245 F. Supp. 319, 321 (D. Mass. 2003).

46. *Id.* at 203.

47. *Id.*

48. *Id.*

49. *Id.* at 204.

50. United States v. Councilman, 385 F.3d 793 (1st Cir. 2004).

51. United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005).

52. *Id.* at 73, *citing* Russello v. United States, 464 U.S. 16, 23 (1983).

53. *Id.* at 75.

54. *Id.*

55. *Id.* at 77.

56. *Id.*

57. *Id.* at 78.

58. *Id.* at 80.

59. 18 U.S.C. § 2511(4)(a) (2005).
60. 18 U.S.C. § 2511(2)(d) (2005).
61. *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 20-21 (1st Cir. 2003). *See also* Williams v. Poulos, 11 F.3d at 281-82 (1st Cir. 1993); Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998).
62. *Id.* at 21.
63. *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).
64. National Conference of State Legislatures (2006), http://www.ncsl.org/programs/lis/CIP/surveillance.htm (last visited September 14, 2005).
65. Dragomir Cosanici, *Email Privacy June 2002*, History, Arts and Libraries, The Official State of Michigan Website, *at* http://www.michigan.gov/hal/0,1607,7-160-17451_18668_18689-54445--,00.html (June 1, 2002).
66. United States v. Marion, 535 F.2d 697, 702 (2d Cir. 1976).
67. *Id* at 702.
68. Cal. Penal Code § 631 (2005).
69. Conn. Gen. Stat. § 52-570d (a) (2004).
70. Del. Code Ann. tit. 11, § 1335(a)(4) (2005).
71. Fla. Stat. ch. 934.03(d) (2005).
72. 720 Ill. Comp. Stat. 5/14-2(1) (2005).
73. Md. Code Ann., Cts. & Jud. Proc. § 10-402(c)(3) (2005).
74. Mass. Gen. Laws ch. 272, § 99(B)(4) (2005).
75. Mich. Comp. Laws § 750.539c (2005).
76. Mont. Code Ann. § 45-8-213(1)(c) (2004).
77. N.H. Rev. Stat. Ann. § 570-A:2 I-a (2004).
78. 18 Pa. Cons. Stat. § 5704(4) (2005).
79. Wash. Rev. Code § 9.73.030(3) (2005).
80. For a general overview of Gmail, *see* Google, What is Gmail? (2006),

http://mail.google.com/mail/help/about.html. For Gmail's privacy policy, *see* Google, Gmail Privacy Notice (2006), http://gmail.google.com/mail/help/privacy.html.

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

<< Top