

COMMONWEALTH OF MASSACHUSETTS

SJC Docket No. 12103

APPEALS COURT Docket No. 2015-P-0901

DEBRA L. MARQUIS,
Plaintiff-Appellant/Cross-Appellee,

v.

GOOGLE INC.,
Defendant-Appellee/Cross-Appellant.

ON APPEAL FROM A FINAL ORDER OF
THE SUFFOLK SUPERIOR COURT

OPENING BRIEF FOR PLAINTIFF-APPELLANT

(REDACTED)

For DEBRA L. MARQUIS,

John Peter Zavez, BBO #555721
Jason B. Adkins, BBO #558560
Jeffrey Thorn, BBO #677222
ADKINS, KELSTON & ZAVEZ, P.C.
90 Canal Street, Suite 500
Boston, MA 02114
(617) 367-1040
jzavez@akzlaw.com
jadkins@akzlaw.com
jthorn@akzlaw.com

Dated: October 2, 2015

TABLE OF CONTENTS

TABLE OF AUTHORITIES..... iii

INTRODUCTION..... 1

ISSUES PRESENTED..... 2

STATEMENT OF THE CASE..... 3

 I. History of the Proceedings 3

 II. Statement of Facts 3

SUMMARY OF ARGUMENT..... 7

ARGUMENT..... 8

 I. Standard of Review 8

 II. The Superior Court Erred in Granting Summary
 Judgment for Defendant 8

 A. The Superior Court Failed to Distinguish between
 the Criminal and Civil Portions of the Act..... 8

 B. The Superior Court Erred in Its Choice of Law
 Analysis..... 10

 C. No Other Arguments Justify the Granting of
 Summary Judgment in Google's Favor..... 16

 III. The Superior Court Erred in Denying Partial
 Summary Judgment (Liability) for Plaintiff 23

 IV. The Superior Court Erred in Denying Plaintiff's
 Motion for Class Certification 27

 A. Plaintiff's Proposed Class 28

 B. Plaintiff's Proposed Class Meets All Criteria
 for Certification 29

 C. The Court Failed to Address the Google Apps
 Subclass 46

CONCLUSION..... 50

ADDENDUMS

- (1) Massachusetts Wiretap Statute
(M.G.L. c. 272, §99)
- (2) Memorandum and Order on Cross-Motions for
Summary Judgment
- (3) Memorandum of Decision and Order on
Plaintiff's Motion for Class Certification
- (4) Certificate of Compliance
- (5) Certificate of Service

TABLE OF AUTHORITIES

FEDERAL CASES

<i>Abelston v. Strong,</i> 1987 WL 15872 (D. Mass. 1987).....	33
<i>Adair v. Sorenson,</i> 134 F.R.D. 13 (D. Mass. 1991).....	35
<i>Andrews v. Bechtel Power Corp.,</i> 780 F.2d 124 (1st Cir. 1985).....	35
<i>BMW of North America, Inc. v. Gore,</i> 517 U.S. 559 (1996)	13
<i>Campiti v. Walonis,</i> 611 F.2d 387 (1st Cir. 1979)	40,41
<i>Duhaime v. John Hancock Mutual Life Ins. Co.,</i> 177 F.R.D. 54 (D. Mass. 1997).....	42,43
<i>Free Speech Coalition, Inc. v. Shurtleff,</i> 2007 WL 922247 (D. Ut. Mar. 23, 2007).....	15
<i>Gilday v. Dubois,</i> 124 F.3d 277 (1st Cir. 1997).....	17
<i>Gintis v. Bouchard Transp. Co., Inc.,</i> 596 F.3d 64 (1st Cir. 2010).....	37,39
<i>In re Prudential Ins. Co. of America Sales Practices,</i> 148 F.3d 283 (3d Cir. 1998).....	36
<i>Kirby v. Cullinet Software,</i> 116 F.R.D. 303 (D. Mass. 1987).....	30
<i>MacNeil Engineering Co., Inc. v. Trisport, Ltd.,</i> 59 F. Supp. 2d 199 (D. Mass. 1999).....	11
<i>Northeast Bancorp, Inc. v. Board of Governors of the Federal Reserve System,</i> 472 U.S. 159 (1985).....	14
<i>Payne v. Goodyear Tire & Rubber Co.,</i>	

216 F.R.D. 21 (D. Mass. 2003).....	36,37
<i>Pendell v. AMS/Oil, Inc.</i> , 1986 WL 5286 (D. Mass.).....	11
<i>Pennsylvania v. Nelson</i> , 350 U.S. 497 (1956).....	14
<i>Randle v. Spectran</i> , 129 F.R.D. 386 (D. Mass. 1988).....	33
<i>Schacter v. Circuit City Stores, Inc.</i> , 433 F. Supp. 2d 140 (D. Mass. 2006).....	24,25
<i>Smilow v. Southwestern Bell Mobile Systems, Inc.</i> , 323 F.3d 32 (1st Cir. 2003).....	38

STATE CASES

<i>Birbiglia v. St. Vincent Hosp., Inc.</i> , 427 Mass. 80 (1998).....	45
<i>Bellerman v. Fitchburg Gas & Elec. Light Co.</i> , 470 Mass. 43 (2014).....	48
<i>Brophy v. School Committee of Worcester</i> , 6 Mass. App. Ct. 731 (1978).....	30,32
<i>Campbell v. Glodis</i> , 28 Mass. L. Rptr. 465 (Mass. Super. Ct. 2011)...	32
<i>Commonwealth v. Armstrong</i> , 73 Mass. App. Ct. 245 (2008).....	9
<i>Commonwealth v. Hyde</i> , 434 Mass. 594 (2001).....	26,27
<i>Commonwealth v. Jackson</i> , 370 Mass. 502 (1976).....	40,41,42
<i>Commonwealth v. Vitello</i> , 367 Mass. 224 (1975).....	13,14
<i>Cosme v. Whitlin Mach. Works, Inc.</i> , 417 Mass. 643 (1994).....	11

<i>Crosland v. Horgan</i> , 401 Mass. 274 (1987).....	16,17
<i>Deutsche Bank Nat. Trust Co. v. Gabriel</i> , 81 Mass. App. Ct. 564 (2014).....	8
<i>District Attorney for Plymouth Dist. v. New England Tel. & Tel. Co.</i> , 379 Mass. 586 (1980).....	24
<i>Fletcher v. Cape Cod Gas Co.</i> , 394 Mass. 595 (1985).....	31
<i>Heffernan v. Hashampour</i> , 26 Mass. L. Rptr. 541 (Mass. Super. 2009)....	10,11
<i>Kwaak v. Pfizer, Inc.</i> , 71 Mass. App. Ct. 293.....	8
<i>New England Tel. & Tel. Co. v. Gordeau Cons. Co., Inc.</i> , 426 Mass. 261 (1997).....	10
<i>O'Sullivan v. NYNEX Corp.</i> , 426 Mass. 261 (1997).....	18,19
<i>Pine v. Rust</i> , 404 Mass. 411 (1989).....	8,9
<i>Ramos v. Registrars of Voters of Norfolk</i> , 374 Mass. 176 (1978).....	36
<i>Rich v. Rich</i> , 28 Mass. L. Rptr. 553 (Mass. Super. July 8, 2011).....	5,27
<i>Spear v. H.V. Greene Co.</i> , 246 Mass. 259 (1923).....	31
<i>Weld v. CVS Pharmacy, Inc.</i> , 11 Mass. L. Rptr. 21 (Mass. Super. Ct. 1999)....	30
<i>Weld v. Glaxo Wellcome, Inc.</i> , 434 Mass. 81 (2001).....	34,37,43

State Statutes

M.G.L. c. 272, § 99.....	<i>passim</i>
--------------------------	---------------

State and Federal Rules

Mass. R. Civ. P. 23.....*passim*

Fed. R. Civ. P. 23.....*passim*

Additional Authority

Smith and Zobel, *Massachusetts Rules*, § 23.4...30,35,37

INTRODUCTION

This appeal arises out of two erroneous holdings by the Superior Court (1) granting summary judgment for defendant and (2) denying class certification.

In granting summary judgment for defendant, the Superior Court held that the Massachusetts Wiretapping Act ("Act") does not apply to Defendant Google Inc.'s "interceptions, disclosures, and use" of Plaintiff's emails exchanged with Gmail users because Google runs the coding for its scanning program on servers physically located outside of Massachusetts. This was error because the Superior Court misapplied the extra-territoriality analysis used for criminal law to civil claims and/or the since-discarded *lex loci delicti* choice of law analysis. Under the correct analysis, the Superior Court should have granted partial summary judgment (liability) on behalf of Plaintiff.

In denying class certification, the Superior Court held that individual issue of whether class members knew their emails were being read predominated over common issues. This was error because the controlling decision holds that a person must have actual knowledge that his specific communications are

being tapped before he can impliedly consent to such tapping, and it is undisputed that no class member knew whether his specific communications are being tapped. Even if the Superior Court correctly applied the controlling case law, it should have still certified a subclass of Massachusetts residents who did not know they were exchanging emails with Google Apps Gmail account holders.

ISSUES PRESENTED

(1) Did the Superior Court err in granting Summary Judgment for Defendant on Plaintiff's claim for civil violation of the Act on the grounds that the Act did not apply to emails sent or received by Massachusetts residents but intercepted outside of Massachusetts, where the Superior Court relied on an erroneous choice of law standard based on criminal choice-of-law analysis and/or a since-rejected civil choice-of-law approach?

(2) Did the Superior Court err in denying Summary Judgment on Plaintiff's Cross-Motion for Partial Summary Judgment (Liability) where it was undisputed that Google had wiretapped/intercepted Plaintiff's emails without her knowledge?

(3) Did the Superior Court err in denying Plaintiff's Motion for Class Certification on the grounds that common issues did not predominate over the individual issue of whether each class member had consented to Google's intercepting his/her emails, where the controlling case law and undisputed facts lead to the inescapable conclusion that no class member could have known that Google was intercepting his/her emails?

STATEMENT OF THE CASE

I. History of the Proceedings

On July 29, 2011, Plaintiff filed her Class Action Complaint. Joint Appendix ("JA") 0006. On January 17, 2012, the Superior Court (Lauriat, J.) denied Defendant's Motion to Dismiss. JA 0013 ("M.T.D. Dec."). On June 19, 2014, the Superior Court (Kaplan, J.) denied Plaintiff's Motion for Class Certification. JA 0935 ("C.C. Dec."). On February 13, 2015, the Superior Court (Billings, J.) denied Plaintiff's Cross-Motion for Partial Summary Judgment and granted Defendant's Motion for Summary Judgment. JA 1653 ("S.J. Dec."). On March 12, 2015, Plaintiff noticed this appeal.

II. Statement of Facts

Plaintiff Deborah Marquis is a resident of

Massachusetts with a non-Gmail email account, i.e., an AOL.com email account. JA 0007. Plaintiff routinely exchanges emails with other person who use Gmail accounts. JA 0007. Plaintiff did not know that Google was intercepting and/or scanning and/or reading her mails exchanged with Gmail users. JA 1065 (Summary Judgment Statement of Fact ("S.O.F.") ¶ 17).

Gmail is an email service owned and operated by Google made available to the general public on February 14, 2007. JA 0022 (Defendant Google Inc.'s Answer to the Complaint ("Ans.") at ¶7). Google raises revenue from Gmail by selling advertisements targeted at Gmail users. JA 0022-23 (Ans. at ¶¶ 2, 8). There are millions of Gmail users in the United States. See JA 1402 (Summary Judgment Joint Appendix ("S.J.") Exh. 38, Rule 30(b)(6) Deposition of Pradeep Kyansur ("Kyansur Dep.") 47:9-10, 46:10.

In order to increase what it can charge for advertisements, Google targets Gmail users with ads that are the most likely to be clicked on and result in a purchase. It does so by intercepting private emails exchanged between Gmail users and non-Gmail users and scanning them for substantive content with a device, JA0023-24 (Ans. at ¶¶ 9 & 11), but without the

prior consent of the non-Gmail users who are Massachusetts residents in violation of M.G.L. c. 272, §99(C)(1).¹ JA 0007 (Compl. at ¶ 2).

In addition, in or around 2007, Google introduced a service called Google Apps, which allowed customer organizations to have their email operated by Google in whole ("pure Gmail") or in part (customers using their own servers in conjunction with Gmail). JA 1387 (Expert Analysis of Michael Helmstadter ("Helmstadter Analysis")) at ¶51. Some Google Apps customers using Gmail do not have "gmail" included in their email address so it is not evident from these emails that the accounts are actually Gmail accounts scanned by Google. See *id.*

Google "intercepts, discloses or uses" (within the meaning of M.G.L. c. 272, §99(Q)²) emails sent both (1) from non-Gmail users to Gmail users and (2) from Gmail users to non-Gmail users, acquires keywords and/or content from non-Gmail users' emails, and then sends

¹ M.G.L. c. 272, §99(C)(1) prohibits interception of wire or oral communications, subject to certain exemptions which do not apply here.

² M.G.L. c. 272, §99(Q) sets forth "civil remed[ies]" available for Massachusetts residents whose wire communications have been "intercepted, disclosed or used."

ads related to those keywords and/or content to the Gmail users. See, e.g., JA 1146 (S.J. Exh. 8). For example, an email exchange between a Gmail user and a non-Gmail user about cars would result in Google displaying an ad for a car manufacturer to that Gmail user. See, e.g., JA 1140, 1153 (S.J. Exhs. 6, 10). These emails are wire communications as defined by M.G.L. c. 272, §99(B)(1).³ JA 0017 (M.T.D. Dec. at 5); see also *Rich v. Rich*, 2011 WL 3672059, * 5 (Mass. Super. Ct. July 8, 2011) (McGuire, J.).

Since roughly [REDACTED], Google has used a new advertising system dubbed "interest-based advertising" and/or "User Modeling." JA 0008 (Compl. at ¶ 11); JA 1067-1070 (S.O.F. ¶¶29-34). Instead of basing advertising solely on keywords found in a single email, as it did originally, Google scans numerous emails exchanged between non-Gmail users and Gmail users for commercial content in order to create a model for providing targeted advertising to the Gmail user. JA 0008 (Compl. at ¶ 11); JA 1067-1070 (S.O.F. ¶¶ 29-34).

³ Wire communications include communications travelling by "the aid of wire, cable, or other like connection." M.G.L. c. 272, § 99(B)(1) (emphasis added).

SUMMARY OF ARGUMENT

Contrary to the Superior Court's holding, see JA 1664 (S.J. Dec. at 12), the Massachusetts Wiretap Act (the "Act") applies to extraterritorial interceptions of emails sent and/or received by Massachusetts residents. (Argument at pp. 9-16.) As a result, the Superior Court erred in denying Summary Judgment on Plaintiff's Cross-Motion for Summary Judgment on Plaintiff's claim for violation of the Act and granting Summary Judgment for Defendant on the grounds that the interceptions took place outside of Massachusetts. Instead, the Superior Court should have granted partial summary judgment (liability) for Plaintiff. (Argument at pp. 23-26.)

Further, in erroneously denying Plaintiff's Motion for Class Certification, the Superior Court abused its discretion by making a clear error of law as to what constitutes a secret interception under the Act as well as errors of fact in asserting that putative class members could know that Google was in fact intercepting their emails. (Argument at pp. 40-42.) Because Plaintiff meets all of the other requirements for certifying the proposed class, this class should have been certified. (Argument at pp.

27-46.) In the alternative, even if the Superior Court was correct on its interpretation of what constitutes a secret interception, it simply failed to address a class consisting of Massachusetts residents exchanging emails with Google Apps users who could not have known they were e-corresponding with Gmail users. (Argument at pp. 46-49.)

ARGUMENT

I. Standard of Review

The standard of review of a grant of summary judgment is de novo. *Deutsche Bank Nat. Trust Co. v. Gabriel*, 81 Mass. App. Ct. 564, 565 n.7 (2014).

The standard of review of a denial of a motion for class certification is abuse of discretion. *Kwaak v. Pfizer, Inc.*, 71 Mass. App. Ct. 293, 297 (2008).

II. The Superior Court Erred in Granting Summary Judgment for Defendant

A. The Superior Court Failed to Distinguish between the Criminal and Civil Portions of the Act

There is a clear distinction between the criminal and civil portions of the Act. See *Pine v. Rust*, 404 Mass. 411, 414 (1989) ("To be actionable under [the civil portion] an interception need not rise to the level of

criminal conduct covered by the penal provisions of the law."). Ignoring *Pine*, the Superior Court erroneously relied on criminal cases to assert that the civil provisions of the Act have no extraterritorial enforcement. See JA 1664 (S.J. Dec. at 12) ("I conclude that the statute does not apply to an interception occurring outside Massachusetts"). The Superior Court concluded:

The statute does not distinguish between conduct that is punishable criminally and that which is subject to civil remedies; an act either is an unlawful interception, or it isn't.

JA 1662 (S.J. Dec. at 10). This was legal error because the Act does distinguish between criminal and civil actions.

The majority rule prohibits extraterritorial enforcement of criminal portion of the Act. See *Commonwealth v. Armstrong*, 73 Mass. App. Ct. 245, 249 (2008) ("The general rule ... is that a State may not prosecute an individual for a crime committed outside its boundaries."). Violations of the Act are criminal only where such violation is "willful" **and** it occurs within Massachusetts. Therefore, under the facts developed here, Google would not face potential criminal liability.

B. The Superior Court Erred in Its Choice of Law Analysis

1. The Superior Court Erroneously Relied on the Doctrine of Lex Loci Delicti

The Superior Court erroneously relied on federal cases involving the civil portion of the Act. See JA 1667 (S.J. Dec. at 15) (citing to 1986 and 1999 decisions). Those cases, in turn, relied upon the *lex loci delicti* (place of the wrong) choice-of-law analysis that has since been rejected by the Supreme Judicial Court and replaced with the Restatement (Second) of Conflicts of Law's two-part analysis. See, e.g., *New England Tel. & Tel. Co.*, 419 Mass. 658, 663-64 (1995); *Cosme v. Whittin Mach. Works, Inc.*, 417 Mass. 643, 646-47 (1994).

Heffernan v. Hashampour, 2009 WL 6361870 (Mass. Super.), applied the current correct Restatement choice-of-law analysis to a case concerning the Act. Under the correct approach, a court must look, first, to which section of the Restatement (Second) of Conflict of Laws was most analogous to the tort alleged. *Heffernan* at *1. The *Heffernan* court found that, for wiretapping, Section 152 (invasion of privacy) was most analogous and thus, under Section 152, a court should apply "local law of the state

where invasion occurred." *Id.* at 2. Per Comment C, the "place of invasion [of privacy] is the place where the plaintiff was at the time." *Id.* Thus, when the correct choice-of-law analysis is conducted, the Act clearly applies to Google's interception of Plaintiff's emails.

Furthermore, *Heffernan* correctly distinguishes the two older federal cases the Superior Court relies upon: *Pendell v. AMS/Oil, Inc.*, 1986 WL 5286 (D. Mass.) (relying upon *lex loci delicti* in choosing Rhode Island wiretapping law over Massachusetts version), and *MacNeil Engineering Co., Inc. v. Trisport, Ltd.*, 59 F. Supp. 2d 199 (1999) (relying on "*Pendell's* choice of law analysis"). See *Heffernan* at *3 n. 6 (noting that "*Pendell*, a non-binding opinion, applied the now-outdated *lex loci delicti* approach"). Because these federal civil cases relied upon a choice-of-law analysis no longer used by Massachusetts state courts, it was error to rely upon them in our case. Under the current, correct analysis, the Superior Court should have held that the Act applied to emails exchanged between Plaintiff and Gmail users.

2. The Superior Court Ignored Clear
Legislative Intent by Basing its
Summary Judgment Decision on the
Possible Consequences of a Ruling in
Favor of Plaintiff

Instead of properly limiting itself to applying the Act, the Superior Court guessed at the future effects of applying the Act to Gmail:

There is no reason to suspect that the Massachusetts legislature intended, in 1968 or since, that our statute be applied to out-of-state conduct, especially where this would amount to a Massachusetts-imposed interdiction against a practice whose implementation occurs elsewhere and whose effects - good and bad - are worldwide.

JA 1668 (S.J. Dec. at 16). This anticipation of such a "Massachusetts-imposed interdiction" is improper because it ignores the Legislature's intent to protect Massachusetts residents from privacy-violating technological innovations such as Defendant's interception of email:

The general court further finds that the **uncontrolled development and unrestricted use of modern electronic surveillance devices** pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the **secret use** of such devices by private individuals must be prohibited.

G.L. c. 272, § 99(A) (emphasis added). If the Superior Court had simply applied the Act as intended, it would have found Google civilly liable.

3. The Court Erred in Applying *BMW of North America, Inc.* to this Case

The Summary Judgment Decision correctly observes that "a State may not impose economic sanctions on violators of its laws with the intent of changing the tortfeasors' lawful conduct in other states. JA 1667 (S.J. Dec. at 16) (citing *BMW of North America, Inc. v. Gore*, 517 U.S. 559, 573 (1996)). Applying the Act to Google, however, does not run afoul of *Gore*. In the portion relevant to this case, *Gore* held only that a defendant's actions that were legal in the states where committed, could not be used in calculating punitive damages in a state where those actions were illegal. *Gore*, 116 S. Ct. at 1597-98; *Gore* at 1613 ("There is no basis for believing that Alabama has sought to control conduct elsewhere.") (Scalia, J. dissenting). Unlike *Gore*, Plaintiff only seeks to hold Google liable for invasions of privacy occurring in Massachusetts (under the correct choice-of-law analysis) against Massachusetts residents.

4. The Act Does Not Violate the Dormant Commerce Clause

Federal wiretapping law does not preempt those portions of the Act relevant here. See *Com. v. Vitello*, 367 Mass. 224, 245 (1975) ("Congress in

enacting Title III intended to occupy the field of wiretapping and electronic surveillance, except as that statute specifically permits concurrent State regulation"); JA 0018 (M.T.D. Dec. at 6). As the Supreme Judicial Court observed, the federal wiretapping statute did not preempt state law related to civil remedies:

the Senate Report on particular provisions on Title III specifically indicates areas in which the Congress did not intend to preempt State legislation. See, e.g., ... recovery of civil damages.

Vitello, 367 Mass. at 245 n.7. The *Vitello* court further noted that it was "indisputable" that Congress "did not intend to supersede State law entirely." 367 Mass. at 249-50; c.f., e.g., *Pennsylvania v. Nelson*, 350 U.S. 497 (1956). And, finally, the *Vitello* court noted:

Title III expressly recognizes that States may ... adopt procedures and standards more restrictive than the Federal act. Thus, the degree of restriction, indeed the very permissibility of wiretapping for law enforcement purposes may differ among States.

367 Mass. at 249-50.

And the dormant commerce clause doctrine does not apply to a field that Congress has chosen not to preempt. See, e.g., *Northeast Bancorp, Inc. v. Board*

of Governors of the Federal Reserve System, 472 U.S. 159 (1985) (not dormant because Congress authorized the state burden); *Free Speech Coalition, Inc. v. Shurtleff*, 2007 WL 922247 (D. Ut. Mar. 23, 2007) at *11 (holding that dormant Commerce Clause does not apply where, e.g., "Congress has expressly allowed states to regulate [interstate] commercial email"). Like this case, *Free Speech* involved the state law regulation of email correspondence with the residents of the regulating state and entities outside of the state.

When Congress passed The Omnibus Crime Control and Safe Streets Act of 1968 (Pub. L. 90-351, 82 Stat. 197, enacted June 19, 1968, codified at 42 U.S.C. § 3711), which included the federal anti-wiretapping statute, telephone lines were in national commerce as much as email connections are today. Because Congress allowed the states to regulate telephone lines by means of state wiretapping laws allowing for "recovery of civil damages," it demonstrated a clear intent not to preempt state regulation of other comparable interstate wire communications (e.g., email) involving civil violations.

**C. No Other Arguments Justify the Granting of
Summary Judgment in Google's Favor**

The Superior Court disregarded Google's other arguments that it had not violated the Act because (1) Google's scanning is not wiretapping since it occurs in the "ordinary course of business"; and (2) the Act only applies to interceptions during transmission. Such arguments are invalid.

1. Ordinary Course of Business

**(i) The "Ordinary Course of its
Business" Exception Only
Applies to Communications
Between Plaintiff and Google
Employees**

Google has argued that it falls under the "ordinary course of business" exception. Massachusetts case law, however, supports Plaintiff's position that the "ordinary course of business" exception only applies when one of the intended communicants is an employee of the entity wiretapping. Google fails to point to a single case where (a) neither communicant was an employee of the wiretapping entity and (b) what would otherwise be a violation of the Act was all the same excused under the "in the ordinary course of business" exception.

Crosland v. Horgan, 401 Mass. 274 (1987), held

the Act had not been violated where, at the direction of a state police officer (who was also the defendant), a hospital employee #1 called another hospital employee #2 while a third hospital employee #3 listened in to determine whether she recognized the voice of hospital employee #2. Not surprisingly, the Supreme Judicial Court concluded that the "ordinary course of business" exception applied to a conversation involving three employees of the same hospital over the hospital's internal phone system. See *Crosland*, 401 Mass. at 276. *Crosland* does not apply to the present case which involves communications between Plaintiff and communicants who are not Google employees, which are in turn intercepted by Google. And *Gilday v. Dubois*, 124 F.3d 277, 288-89 (1st Cir. 1997), held only that the Act had not been violated where plaintiffs had prior knowledge that their calls would be monitored for purposes of "call detailing," i.e., itemized phone bills.

(ii) Google Misinterprets the Superior Court's Holding and Cannot Rely on Cases Where None of the Intended Communicants Were Employees of the Wiretapping Entity

In the M.T.D. Dec., the Superior Court held that

"Google's reliance is misplaced, as it does not have an employer-employee relationship with Google users." JA 0020 (M.T.D. Dec. at 8). This Order properly concluded that Google could not rely upon cases where one of the communicants was an employee of the alleged wiretapping party. Nevertheless, Google's summary judgment briefing relied entirely on cases where one (or more) of the communicants was an employee of the wiretapping party, or the party alleging wiretapping had prior knowledge of the wiretap. See, e.g., *supra* at §II.B.1. These cases are simply inapposite.

**(iii) Google is Not Entitled to an
M.G.L. c. 272, § 99(B)(3) Exemption
Because Its Wiretapping
Hardware/Software is NOT "being used
by a communications common carrier
in the ordinary course of its
business"**

O'Sullivan v. NYNEX Corp., 426 Mass. 261 (1997), makes clear that Google's wiretapping of emails between private parties is not "being used by a communications carrier in the ordinary course of its business." First, because Google is not a "communications common carrier" within the meaning of the Act, see *infra* at §III.B.6, none of its equipment qualifies. Cf. *NYNEX*, 426 Mass. at 265-66 (concluding that telephone equipment used by a telephone company

is exempt). Second, even if Google's equipment can be considered that of a "communications common carrier," the manner in which Google uses such equipment precludes it from being exempt. "The general rule is that monitoring business calls is legal, but eavesdropping on private calls is illegal unless there is a 'legitimate business purpose' for the employer to monitor an employee's conversation." *NYNEX*, 426 Mass. at 265-66. Google fails *NYNEX* on both counts because it is intercepting private calls not involving employees. Third, intercepting emails is not within "its ordinary course of business" as intended by the Act because wiretapping can only be exempt if necessary to the safe and secure operation of the system, not as an end in itself. See *NYNEX*, 426 Mass. at 267 (noting that information obtained was limited to business-related conversations with defendant's own employees and access to such conversations was tightly controlled).

**(iv) Contrary to What Google Argues, the
Wiretap Act Expressly Prohibits
Google from Raising Revenue from
Intercepted Communications**

Google scans/reads the substantive content of emails exchanged with Gmail users and then uses that

information in order to sell targeted advertising to various companies. Doing so is a clear violation of the Civil Remedy portion of the Act, which provides that "Any aggrieved person whose ... property interests ... were violated by means of an interception ... shall have a civil cause of action...." M.G.L. c. 272 § 99(Q). Put simply, Google is violating the Act by selling the information contained in Plaintiff's emails exchanged with Google users, which information is Plaintiff's property.

**(v) There is No Massachusetts Case
Authorizing Google to Intercept
Emails for the Purposes of Selling
Targeted Advertising**

At the Superior Court level, Google has asserted that (a) some email mailbox providers scan emails for purposes unrelated to gaining information for selling targeted advertising and (b) some email mailbox providers display advertising to their email users. JA 1066 (S.O.F. 23, 24). Google then has argued that (a) plus (b) somehow indicates that is a common industry practice for email mailbox providers to scan emails for the purposes of selling target advertising. JA 1278-79 (S.J. Exh. 28 at ¶ 55)

The critical difference is that, even under

Google's asserted facts, most other email mailbox providers do not rely upon reading emails with a third party to determine which ads to show their users. Instead they use voluntarily provided information from their own user, or show non-individualized advertising likely to have broad appeal. For example, Microsoft shows ads based on its own user's web actions, demographic data provided by its own user at registration, and "general interests." JA 1278 (S.J. Exh. 28 at ¶53).

(vi) Google is NOT a "Communications Common Carrier" Because, Unlike Comcast and Verizon, It Does Not Carry Communications for other Email Providers

In erroneously arguing that it is a "communications **common** carrier," Google conveniently ignores the word "common." Companies like Verizon and Comcast are "communications **common** carriers" precisely because they carry communications over a common communications system for other email providers such as Google and Yahoo. For example, Verizon and Comcast carry communications between unrelated entities such as Google and Yahoo, while Google only carries communications involving a Gmail user as one of the communicants.

**2. Google Cannot Escape Liability By
Arguing that It Does Not "Intercept"
Emails During Transmission**

Google argues that some (but not all) of its scanning of emails does not occur during the transmission of the email, and is therefore exempt from the Act. This is incorrect.

The Act defines "interception" as broadly as possible to mean "to secretly hear, secretly record ...the contents of any oral or wire communication through the use of any intercepting device by any person...." M.G.L. c. 272 § 99(B)(4) (emphasis added). The Act similarly defines wire communication as broadly as possible: "The term 'wire communication' means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." M.G.L. c. 272, § 99(B)(1).

Given the realities of email, however, the "point of reception" is when the intended recipient actually opens and views the email, which occurs after the illegal scanning occurs. See, e.g., JA 0986 (Google Mem. in Support of Motion for Summary Judgment at 17

and 17, n.18) ("Google's 30(b)(6) witness ... testified that [REDACTED] scanning [REDACTED] [REDACTED]"); see also JA 1137 (JA Exh. 5 at 102:9-15).

III. The Superior Court Erred in Denying Partial Summary Judgment (Liability) for Plaintiff

There is no dispute that Google intercepted and/or scanned and/or read Plaintiff's email correspondence with Gmail users without her knowledge or consent. JA 1065 (SOF ¶17). Nevertheless, the Superior Court granted summary judgment for Defendant and denied it for Plaintiff based on its erroneous interpretation of the Act. Correct interpretation of the Act compels the opposite conclusion that Plaintiff is entitled to summary judgment.

Google secretly intercepts and reviews emails between private individuals for the purpose of determining the content of their communications. Google does this in order to target advertising at Gmail users for Google's own monetary gain. Google expressly admits that it applies automated systems to scan the texts of Gmail messages for monetary gain. JA 0972 (Google Memo in Support of S.J. at 3). Google also admits that those scanned "texts of Gmail

messages" include the email content received from non-Gmail account holders such as the Plaintiff. See JA 1059-60 S.O.F. ¶2 (Google stating that it "applies automated processing and scanning of emails in Gmail in order to provide ... targeted advertising based on the content of emails"); JA 1061 (S.O.F. ¶5) (same); see also JA 1067-68 (S.O.F. ¶¶ 25-27).⁴

Google secretly scanned Plaintiff's emails without her knowledge or consent. See JA 1065 (S.O.F. ¶ 17); JA 0008, JA 00010 (Compl. ¶¶ 14, 27). Nor was there any reason Plaintiff should have known that Google was secretly scanning her emails. She neither knew, nor should have known, whatever information Google claims to have posted on its website concerning its reading of emails. Plaintiff did not have a Gmail account and therefore had no reason to visit its website to learn its terms. See, e.g., *Schacter v.*

⁴Google has further violated the Act by scanning the header information on emails exchanged between Plaintiff and Gmail users. See *Dist. Att. for the Plymouth Dist. v. New England Telephone & Telegraph Co.*, 379 Mass. 586 (1980). Google is not entitled to the "ordinary course of business exception" here because Google admits that it scans email header information for purposes unrelated to the delivery of email. See, e.g., JA 1108 (S.J. Exh. 3, Kapadia Decl., ¶29) (noting Google scans more than the "text" of the email).

Circuit City Stores, Inc., 433 F. Supp. 2d 140, 144 (D. Mass. 2006) (holding that plaintiff could not be charged with knowledge of additional contract terms posted on defendant's website where plaintiff did not have to agree to those terms before using the product).

Plaintiff could - and did - use her AOL email account to communicate with Gmail account holders without having any further involvement with Google. The Court has previously concluded that Plaintiff adequately alleged that she lacked knowledge of Google's scanning. JA 0020 (M.T.D. Dec. at 8). Google has not since challenged that lack of knowledge. In fact, Google concedes Plaintiff did not learn of Google's scanning, even in a general sense, until July 2011. JA 1065 (S.O.F. 17).⁵ Google has admitted that it has no reason to believe that Plaintiff was aware of its scanning. *Id.*

The Legislature clearly intended for the Act to be read broadly and to be mandatory:

The general court further finds that the uncontrolled development and unrestricted use

⁵Not surprisingly, Google fails to show that it has done anything affirmative to alert non-Gmail account holders such as Plaintiff that her emails are being secretly scanned.

of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. **Therefore, the secret use of such devices by private individuals must be prohibited.**

272 M.G.L. c. § 99(A) (emphasis added). And intended further that the Act must be applied in civil cases to protect Plaintiff and similarly situated Massachusetts residents:

Any aggrieved person whose oral or wire communications were intercepted, disclosed or used **except as permitted or authorized by this section** or whose personal or property interests or privacy were violated by means of an interception except as permitted or authorized by this section **shall have a civil cause of action.**

272 M.G.L. c. § 99(Q) (emphasis added). Given that Plaintiff has satisfied the factual elements of her claim, Google must establish - or at least raise - a plausible exception to the Act. As addressed above, *see supra* at §II.C, Google cannot satisfy any of these exceptions.

Where a defendant cannot satisfy the existing exceptions, the Massachusetts courts will not create new exceptions. *See, e.g., Com. v. Hyde*, 434 Mass. 594, 598 ("The statute is carefully worded and unambiguous and lists no [additional] exception [as defendant argues]. . . . We have no doubt that the

plain language of the statute accurately state's the Legislature's intent."); see also *Rich v. Rich*, 28 Mass. L. Rptr. 553, *4 (2011) ("The Massachusetts Wiretap Act prohibits the interception of oral or wire communications, except pursuant to a duly issued warrant or in **other limited circumstances.**") (emphasis added). Because it cannot rely upon any statutory exceptions, Google is civilly liable under the Act for intercepting and/or scanning and/or reading Plaintiff's emails.

IV. The Superior Court Erred in Denying Plaintiff's Motion for Class Certification

The Superior Court abused its discretion in denying Plaintiff's Motion for Class Certification. First, the Court made a clear error of law as to what constitutes a secret interception under the Act. Second, the Court failed to certify a subclass of non-Gmail emailers who emailed with individuals using Google Apps for email, which uses Google's Gmail system but email addresses do not include "Gmail." Plaintiff raised a Google Apps subclass in her briefing and arguments that neither Defendant rebutted nor the Court substantively addressed.

A. Plaintiff's Proposed Class

Plaintiff sought certification of a class consisting of:

all Massachusetts residents who (1) did **not** have Gmail accounts at the time that they (2)(a) sent emails from their non-Gmail account email accounts to a Gmail account and/or (2)(b) received emails from a Gmail account (3) which emails Google scanned for their substantive content to use for its own commercial purposes (4) at any time from April 2004 (when Google first introduced Gmail) to the present (the "Class"), and are therefore due damages and injunctive relief under the Massachusetts Wiretapping Act, M.G.L. c. 272, §99 (the "Wiretap Act"), from Defendant Google Inc.

JA 0037 (Plaintiff's Motion for Class Certification ("Mot. For C.C.") at 1). Plaintiff explained that "[t]he relevant emails fall into the following separate, distinct and identifiable categories":

- All Class Members' emails that have Smart Labels associated with them regardless of whether the actual email still exists on the Gmail system.
- All emails sent from a Class Member's non-Gmail account to a Gmail account since August 2010, when Google started scanning all incoming email for commercial purposes.
- All emails sent from a Class Members' non-Gmail account to a Gmail account prior to August 2010 that was opened by the Gmail account holder using Google's Web-Based Interface/SMTP pathway.
- All emails sent from a Gmail account using Google's Web-Based Interface/SMTP pathway to a Class Member's non-Gmail account [after August 2010].

- The above 4 categories [which] also apply to emails sent to/from Google Apps customers using pure Gmail for their email.

JA 0474-0475 (Mem. In Support of C.C. at 6); see also JA 0929-30 (Reply in Support of C.C. at 8-9) and JA 0933-34 (Proposed Order at Exh. A).

B. Plaintiff's Proposed Class Meets All Criteria for Certification

In addition to meeting the predominance requirement, Plaintiff meets all of the other requirements set forth in Mass. R. Civ. P. 23(a) and 23(b) for certifying the proposed class.

1. Plaintiff Meets All Criteria of 23(a)

Mass. R. Civ. P. 23(a) establishes four requirements for maintaining a class action: (1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims of the representative parties are typical of the class; and (4) the representative parties will fairly and adequately represent the interests of the class. The proposed Class satisfies all these requirements.

(i) Numerosity

Mass. R. Civ. P. 23(a)(1) requires that a class must be so large that it would be "impractical, unwise

or imprudent" to join all members. *Brophy v. School Comm. of Worcester*, 6 Mass. App. Ct. 731, 735 (1978). It is not necessary that it be "impossible" to join all the members of the class, but simply that it would be unduly difficult, costly, or inefficient to do so. *Id.*; see also Smith and Zobel, *Massachusetts Rules*, § 23.4, 7 M.P.S., 96-97. "A court may make 'common sense assumptions in order to support a finding of numerosity.'" *Weld v. CVS Pharmacy, Inc.*, 11 Mass. L. Rptr. 21, 1999 WL 1565175 (Mass. Super. Ct. 1999) (Brassard, J.) (quoting *Kirby v. Cullinet Software*, 116 F.R.D. 303, 306 (D. Mass. 1987)). Furthermore, the party seeking class certification need only provide sufficient information for the court to make a reasonable judgment as to the numerosity requirement. *Weld*, 434 Mass. at 87.

That common sense approach to numerosity is easily met here. According to ComScore's market share data, in February 2011 Yahoo Mail had approximately 90,000,000 U.S. users, Gmail had approximately 52,000,000, Hotmail had approximately 42,000,000, and AOL had approximately 25,000,000. JA 0477. Assuming that the webmail market share proportions for the United States are reflected in Massachusetts, there

are about 1,891,720 Yahoo accounts, 1,092,994 Gmail accounts, 882,803 Hotmail accounts, and 525,478 AOL accounts held by Massachusetts residents. Moreover, there are hundreds of thousands of additional Massachusetts residents with other non-Gmail accounts, from providers such as Comcast and Verizon. Because the number of Massachusetts residents with non-Gmail email accounts likely numbers in at least the tens of thousands, and given the ubiquity of Gmail accounts with which they inevitably correspond, the Class easily meets the numerosity requirement.

(ii) Commonality

Rule 23(a)(2) requires that there be questions of law or fact common to the class. Total commonality is not necessary. In *Fletcher v. Cape Cod Gas Co.*, the Supreme Judicial Court recognized that courts have "given permissive application to the commonality requirements." 394 Mass. 595, 606 (1985) (citations omitted). Plaintiffs need only demonstrate that "the persons whom they profess to represent have a common interest in the subject matter of the suit and a right and interest to ask for the same relief." *Spear v. H.V. Greene Co.*, 246 Mass. 259, 266 (1923). The commonality requirement is satisfied where the Class

members share those circumstances material to the dispute. *Brophy*, 6 Mass. App. Ct. at 736 (1978); see *Campbell v. Glodis*, 28 Mass. L. Rptr. 465, *3 (Mass. Super. Ct. 2011) (finding commonality where defendant's "alleged policy and/or practice" was common to all plaintiffs despite implementation under varying individual circumstances).

Here, the focus of the litigation is a challenge to Google's policy of scanning the text of emails sent to or from non-Gmail users who are Massachusetts residents. All Class Members have been subjected to this practice, and Plaintiff seeks the same injunctive, declaratory, and monetary/or relief for all Class Members. Some of the common questions of law and/or fact are as follows:

- (1) Whether Google "intercepted, disclosed or used" wire communications made by Plaintiff and the other members of the putative Class;
- (2) Whether Plaintiff and the other members of the putative Class are entitled to recover statutory damages;
- (3) Whether Plaintiff and the other members of the putative Class are entitled to equitable relief prohibiting Google from "intercepting, disclosing or using" their emails in the future, and disgorging all the information it currently wrongfully possesses about Class Members.

(iii) **Typicality**

Mass. R. Civ. P. 23(a)(3) requires that claims of named plaintiffs are typical of the claims of the class. Massachusetts courts have noted that "the burden on plaintiffs in proving typicality is not 'very substantial.'" *Abelson v. Strong*, 1987 WL 15872 at *2 (D. Mass. 1987) (citations omitted). "When it is alleged that the same unlawful conduct was directed at or affected both the named plaintiff and the class sought to be represented, the typicality requirement is usually met irrespective of varying fact patterns which underlie individual claims." *Newberg*, *supra* at § 3-13. As Judge Keeton explained, the question is simply whether a named plaintiff, in presenting his case, will necessarily present the claims of the absent plaintiffs. *Randle v. Spectran*, 129 F.R.D. 386, 391 (D. Mass. 1988) (citations omitted).

Here, there is no divergence between the claims of the Named Plaintiff and the claims of the proposed Class because Marquis and all other Class Members were subject to precisely the same Google corporate practice of intercepting their emails to and from Gmail users without their consent. Plaintiff is an America-On-Line (AOL) email account holder (*i.e.*, non-

Gmail account holder) who has had and continues to have an AOL email account since in or around the late 1990s. JA 0008 (Compl. at ¶ 13). Plaintiff, as well as other Class Members, did not consent to Google's scanning of her emails. JA 0008 (Compl. at ¶ 12). Google, however, has used its proprietary technology to secretly scan emails that Plaintiff, as well as other Class Members, has exchanged with Gmail users. JA 0008 (Compl. at ¶ 14). In such a situation, where there is:

a sufficient relationship ... between the injury to the named plaintiff and the conduct affecting the class [] and the claims are based on the same legal theory ... this alignment of claims and legal theories ensures that the named plaintiff, in "pursu[ing] his or her own self-interest ..., will advance the interests of the class members.

Weld, 434 Mass. at 87 (internal citations omitted).

(iv) Adequacy of Representation

Mass. R. Civ. P. 23(a)(4) requires that named plaintiffs fairly and adequately represent the interests of the class. The court must: (1) determine that the named plaintiffs and their counsel have the ability and incentive to litigate the case; and (2) ensure that the named plaintiffs and their counsel are seeking the ultimate outcome or relief desired by the

proposed Class Members. Smith and Zobel, *supra*, § 23.7, at 99-100 (1975); see also *Adair v. Sorenson*, 134 F.R.D. 13, 18 (D. Mass. 1991) (*quoting Andrews v. Bechtel Power Corp.*, 780 F.2d 124, 130 (1st Cir. 1985)). Both components have been satisfied in this case.

First, the Named Plaintiff and her counsel have the ability and incentive to litigate the case. Plaintiff's counsel - the firm of Adkins, Kelston & Zavez, P.C. - are skilled and experienced practitioners with a record of success in class action litigation. See JA 0511 (Thorn Aff. at Exh. 3).

Second, the Named Plaintiff has sought only the same relief for herself as she has for the proposed Class: statutory damages and declaratory relief ordering the termination of the corporate practice at issue here. Such identicality of relief assures the most vigorous of representation. See, e.g., *Adair*, 134 F.R.D. at 18 (finding proposed class representative adequate because of the "'absence of potential conflict between the named plaintiff and the class members'") (*quoting Andrews v. Bechtel Power Corp.*, 780 F.2d 124, 130 (1st Cir. 1985)).

2. The Proposed Class Satisfies the Requirements of Rule 23(b)

Mass. R. Civ. P. 23(b) imposes two additional requirements upon Massachusetts class actions. First, questions of law or fact common to members of the class must be found to predominate over questions affecting only individual members. Second, a class action must be found superior to other available methods for the fair adjudication of the controversy.

(i) Common Issues Predominate over Individual Issues

Predominance is satisfied where those questions a court need consider concerning the proposed class outweigh those questions concerning individual members of that class. *Ramos v. Registrars of Voters of Norfolk*, 374 Mass. 176 (1978); *Smith & Zobel*, at § 23.8. "A 'single, central issue' as to the defendant's conduct vis-à-vis class members can satisfy the predominance requirement even when other elements of the claim require individualized proof." *Payne v. Goodyear Tire & Rubber Co.*, 216 F.R.D. 21, 27 (D. Mass. 2003) (quoting *In re Prudential Ins. Co. of America Sales Practices*, 148 F.3d 283, 314 (3d Cir. 1998)). The *Payne* court reached the identical conclusion that common issues

predominated over individual issues where, if the class was not certified, each plaintiff would be forced to litigate defendant's liability for virtually identical conduct vis-à-vis each proposed class member. *Payne*, 216 F.R.D 21; see also *Gintis v. Bouchard Transp. Co., Inc.*, 596 F.3d 64 (1st Cir. 2010).

In fact, in similar cases, where defendants have engaged in a "single course of conduct," Massachusetts courts have asserted that predominance is assured, and class certification appropriate:

Because the alleged injuries were the result of the single course of conduct engaged in by CVS and the other defendants, the determination whether the program violated [relevant statutes], or involved a tortious misappropriation for commercial gain of the customers' personal information will turn largely on common questions of law and fact regarding the duty CVS owed to its customers and the defendants' conduct in implementing the program.

Weld, 434 Mass. at 91.

Here, Plaintiff alleges that Defendant has engaged in a "single course of conduct" relevant to liability, and affecting all proposed Class Members in exactly the same manner (though to varying monetary amounts). See *id.* at 92 (class action concerning singular business program concerning customer personal

information turns "largely on common questions of law and fact regarding the duty ... owed and the defendants' conduct in implementing the program" and warrants certification).

Common issues of law and fact predominate because the emails at issue here had their substantive content scanned by Google for its own commercial purposes. When Google scans the contents of incoming non-Gmail for key words to use for targeted advertising, that is the legal equivalent of Google wiretapping a phone call made from a Class Member to a Gmail user. And when Google scans the contents of outgoing Gmail emails to Class Members for key words that it can use for targeted advertising, that is the legal equivalent of Google wiretapping a phone call made by a Gmail user to a Class Member.

Common issues predominate when the key elements of the proposed class's claim can be determined on a class-wide basis. See, e.g., *Smilow v. Southwestern Bell Mobile Systems, Inc.*, 323 F.3d 32, 40 (1st Cir. 2003) (citing numerous cases). As the First Circuit recently stated: "we can say that plaintiffs presented substantial evidence of predominating common issues that called for a searching evaluation." *Bouchard,*

596 F.3d at 66. Justice Souter wrote further for the Court that:

[O]n remand, the focus will be on the plaintiffs' claim that common evidence will suffice to prove injury, causation and compensatory damages for at least a very substantial proportion of the claims that can be brought by putative class members. The proffer of common evidence goes beyond Bouchard's admission of negligence in causing the spill, and includes the contamination and clean-up records that will be offered to show harm to individual ownership parcels... But Bouchard's very opposition to the use of the arguably helpful records seems to promise that most or all cases, if individually litigated would require repetitious resolution of an objection by Bouchard that is common to each one of them.

Bouchard, 596 F.3d at 67.

The Class here meets the predominance requirement because (virtually) all of the elements of Plaintiff's claim are common. This is most easily summarized in the following chart:

<u>Elements of M.G.L. c. 272, §99 Claim</u>	<u>How Determined</u>
---	-----------------------

Google is a "person"	Determined on a class-wide basis
Plaintiffs are "aggrieved persons"	Determined on a class-wide basis
Google "intercepts" email	Determined on a class-wide basis
Google "discloses" email	Determined on a class-wide basis
Google "uses" email	Determined on a class-wide basis
Google acted willfully or knowingly	Determined on a class-wide basis

Plaintiffs entitled to punitive damages	Determined on a class-wide basis
Plaintiffs entitled to injunction	Determined on a class-wide basis
Plaintiffs entitled to statutory damages	Determined on a class-wide basis
Plaintiffs entitled to attorneys' fees	Determined on a class-wide basis

Predominance is satisfied with respect to damages because damages can be calculated on a class-wide basis under a simple formula. The Act entitles each Class Member or "aggrieved person" to recover "liquidated damages computed at the rate of \$100 per day for each day of violation or \$1,000, whichever is higher." 272 M.G.L. c. § 99(Q)(1).

**(ii) The Superior Court Misinterpreted
Commonwealth v. Jackson in
Concluding that Individual Issues
(Class Members' Knowledge)
Predominated over Common Issues**

The Superior Court made a clear error of law by misinterpreting *Commonwealth v. Jackson*, 370 Mass. 502 (Mass 1976) and *Campiti v. Walonis*, 611 F.2d 387 (1st Cir. 1979) (applying *Jackson*), which held that a caller (or, here, the non-Gmail correspondent) had to have actual (not constructive) knowledge that each of his/her particular communications was being intercepted. The question of whether Class members

knew that Google was reading their emails can be determined on a Class-wide basis because knowledge of such wiretapping must be actual knowledge and no Class member could have actual knowledge of whether Google was scanning their emails.

In *Jackson*, 370 Mass. at 507, the Supreme Judicial Court held that "the caller needs to have actual knowledge of the recording, but we believe that actual knowledge is proved where there clear and unequivocal objective manifestations of knowledge...." The Court then held that actual knowledge had been proved only where the defendant/caller had said during the course of the conversation "that he knew the telephone was tapped." *Jackson*, 370 Mass. at 505. Even though a kidnapper such as Jackson might suspect that his calls to the victim's home would be tapped - e.g., because victims' phones are typically tapped in hopes of catching the kidnapper - such suspicions did not constitute actual knowledge and such wiretapping was still secret and therefore in violation of the Act.⁶ See *Campiti*, 611 F.2d at 396 (noting that

⁶ Even though defendant Jackson said during the first and third calls that he knew he was being wiretapped, the Supreme Judicial Court concluded that the second, fourth and fifth calls violated the Act because

communications in *Jackson* where defendant did not speak of being tapped were correctly excluded for violating the Act and thus rejecting the defense that "the intercept was not secret because [plaintiff] should have known that he would be monitored fails").

Applying *Jackson* to Plaintiff's case, even those Class members who were aware that Google scans some emails would not have actual knowledge of whether Google would scan any particular email because, as Google concedes, Google only scans certain emails, JA 0526 (Google C.C. Opp. at 6-7), and the criteria for Google's determination of whether to scan a particular email is not public knowledge. JA 0535-37 (Google C.C. Opp. at 15-17). Therefore, Google's scanning of all of Class members' emails is "secret" within the meaning of the Act non-Gmail users could not know whether Google was intercepting their emails.

(iii) Superiority of Class Action

Finally, Mass. R. Civ. P. 23(b) requires that a class action be superior to other available forms of litigation. A class action is superior where it would promote economies of time, effort and expense, and

Jackson did not say that he knew those specific calls were being wiretapped. See *Jackson*, 370 Mass. at 504.

uniformity of decision. *Duhaime v. John Hancock Mutual Life Ins. Co.*, 177 F.R.D. 54, 65 (D. Mass. 1997). A "case presents a classic illustration of the policies of judicial efficiency and access to courts that underlie the consumer class action suit [when] it aggregates numerous small claims into one action, whose likely range of recovery would preclude any individual plaintiff from having his or her day in court." *Weld*, 434 Mass. at 93.

As Justice Souter noted in a similar context, "Given the elements of injury, causation and compensation on which [Defendant] intends to join issue, there is a real question whether the putative class members could sensibly litigate on their own for these [stated] amounts of damages, especially with the prospect of expert testimony required." *Bouchard*, 596 F.3d at 68. Here, similar circumstances demonstrate the superiority of litigation of these claims as a class action. The Class is so numerous as to make joinder highly "impracticable."

With Class Members likely numbering in the millions and potentially relevant emails into the tens of millions, it would be highly inefficient to litigate each member's claims separately. After all,

all of the computer programming necessary to validate the Class representative's individual claim can be scaled to validate every other Class Members' claim at the same time. A class action is far superior to trying identical individual case millions of times or, what is more likely, denying most affected Massachusetts residents the opportunity to ever have their claims resolved on the merits. Given the small size of each individual Class Member's claim relative to the expense of litigating it, a class action is the only realistic opportunity for each affected Massachusetts resident to vindicate his/her rights. A class action is especially superior in circumstances like the ones here, where affected Massachusetts residents do not even realize that Google is scanning the substantive content of their emails for its own commercial purposes.

Specifically, a jury trial here would focus on the issue of whether it is a violation of the Act for Google to scan the substance of a Massachusetts residents' email correspondence with a Gmail user for Google's own mercantile purposes (*i.e.*, Google selling targeted advertising) that have nothing to do with maintaining the security and/or integrity of the Gmail

system.⁷ The Class Representative would put on evidence showing that Google had scanned her emails sent to Gmail accounts and/or Gmails that she had received, as well as the emails sent and received by other Class Members, and that Google had done that scanning for its own mercantile purposes that had nothing to do with spam blocking or virus prevention, network security or operational reasons. If the Class Representative succeeds in showing that Google had violated the Act with respect to these emails, then the Court will order that the Class be given notice of the decision and each Class Member be allowed to file a claim (form) with an independent claims administrator appointed by this Court.

Furthermore, Plaintiff does not envision any difficulties in the management of the case as a class action that would not be outweighed by the benefits of resolving the Act claims of millions of Massachusetts residents in a single proceeding. Because the controlling law is a Massachusetts statute, the Court is the ideal forum for resolving this controversy.

⁷ See *Birbiglia v. St. Vincent Hosp., Inc.*, 427 Mass. 80 (1998) (plaintiff entitled to jury trial on claims brought under Massachusetts Wiretap Statute).

Because the evidence establishing Defendant's liability would be virtually identical for each Class Member, litigating this case as an individual action would involve nearly as much discovery and preparation as litigating on a class-wide basis. Therefore, judicial economy weighs heavily in favor of class certification.

C. The Superior Court Failed to Address the Google Apps Subclass

1. Plaintiff Timely Raised the Google Apps Subclass

In denying class certification, the Superior Court declined to address the Google Apps subclass:

it is inappropriate to raise this new subclass issue in a letter delivered to the court after the parties have filed their memoranda and evidentiary materials. This is particularly inappropriate when the question is no longer certification of subclasses, but rather whether this proposed subclass will be the only class certified.

JA 0962 (C.C. Dec. at 28). The Court's finding that Plaintiff had "raise[d] this new subclass issue in a letter delivered to the court after [briefing and arguments]" constituted clear error.

In her motion for class certification, Plaintiff set forth the proposition that Defendant's scanning of emails applied not only to emails exchanged with

"gmail.com" email addresses, but also to emails exchanged with Google Apps customers. See JA 0475 (C.C. Mem. at 6, bullet point 5) ("The above 4 categories also apply to emails sent to/from Google Apps customers using pure Gmail for their email."). In her reply, Plaintiff again set forth the appropriateness of such a subclass:

Emails sent to/from Google Apps customers using pure Gmail for their email that satisfy the criteria of any of the above four categories. Based on: Thorn Aff. Exh. 2 Helmstadter Analysis III.A (¶¶26-34).

JA 0933-34 (Proposed Order at Exh. A); JA 0929-30 (Reply in Support of C.C. at 8-9) (describing "Category 5: Emails between Class Members and Google Apps users using pure Gmail.").

At Oral Arguments, Plaintiff again raised this very issue of Google Apps. JA 1721 (Tr. of Mot. Hr'g Dated April 3, 2014 at 51:1-10). The Court then stated, directly and explicitly, "I suppose we could certify a class of ... everybody that has communicated with a Google Apps client as to who confidentiality has been maintained... ." JA 1725 (Tr. Of C.C. Mot. H'rg (55:6-9)).

Finally, in the letter to the Court dated April 9, 2014 (which the Court referenced in its C.C. Dec. at JA 0962), Plaintiff then reiterated to the Court, after Oral Arguments, that Defendant's arguments - concerning consent and Google's public disclosure of its scanning - failed to address scanning of emails to Defendant's email addresses which (intentionally) omitted "Gmail" or "Google" identifiers.

The Supreme Judicial Court has stated that:

Where a natural alternative class or set of subclasses would address a judge's concerns about certifying a class as initially proposed, the judge should redefine the original class or certify subclasses as appropriate.

Bellermann v. Fitchburg Gas & Elec. Light Co., 470 Mass. 43, 58 (2014).

2. Defendant Has Never Denied the Substantive Validity of this Subclass

Even if the Superior Court was correct in its interpretation of what constitutes a (secret) interception, it failed to address a class consisting of Massachusetts residents exchanging emails with Google Apps users.

With this category of emails, even if a Class member knew that Google would read his/her emails exchanged with an email account with an "@gmail.com"

suffix, Class members may also exchange emails with Google Apps clients who are using Gmail for their email without having an "@gmail.com" suffix. For example, if Fictitious University is a Google Apps client, its students will use an email suffix like "Jane.Doe@FictitiousU.edu," instead of "Jane.Doe@gmail.com" so that the Class member will not know that Jane Doe is a Gmail user.

In fact, the list of Google Apps clients is so secret that Google has never produced a full list to the Plaintiff here on the grounds of confidentiality. See JA 1724 (Tr. Of C.C. Mot. H'rg (55:6-9). Google admits, however, that it can identify Google Apps accounts. JA 0495 (Google Rule 30(b)(6) Dep. (Pradeep Kyansur) at 59:10-12) (agreeing a Gmail account "can be identified as a Google Apps account or a non-Google Apps account").

Therefore, if the Appeals Court is not inclined to certify the Class as originally defined, certification of a Google Apps subclass (consisting of Massachusetts residents without Gmail accounts who exchanged emails with Google Apps clients without "Gmail" in their email addresses) would be appropriate.

CONCLUSION

Plaintiff/Appellant requests that the Appeals Court: (1) overrule the Superior Court's order granting summary judgment in favor of Google and grant partial summary judgment (liability) in favor of Plaintiff and (2) overrule the Superior Court's denial of class certification and grant class certification (a) on behalf of the originally defined class; or (b) in the alternative, on behalf of a class of non-Gmail users who have communicated with users of Google Apps.

Respectfully submitted for the
Plaintiff-Appellant,



ADKINS, KELSTON & ZAVEZ, P.C.
John Peter Zavez, BBO #555721
Jason B. Adkins, BBO #558560
Jeffrey Thorn, BBO #677222
90 Canal Street, Suite 500
Boston, MA 02114
(617) 367-1040
jzavez@akzlaw.com
jadkins@akzlaw.com
jthorn@akzlaw.com

Dated: October 2, 2015

Massachusetts General Laws Annotated
Part IV. Crimes, Punishments and Proceedings in Criminal Cases (Ch. 263-280)
Title I. Crimes and Punishments (Ch. 263-274)
Chapter 272. Crimes Against Chastity, Morality, Decency and Good Order (Refs & Annos)

M.G.L.A. 272 § 99

§ 99. Interception of wire and oral communications

Currentness

Interception of wire and oral communications.--

A. Preamble.

The general court finds that organized crime exists within the commonwealth and that the increasing activities of organized crime constitute a grave danger to the public welfare and safety. Organized crime, as it exists in the commonwealth today, consists of a continuing conspiracy among highly organized and disciplined groups to engage in supplying illegal goods and services. In supplying these goods and services organized crime commits unlawful acts and employs brutal and violent tactics. Organized crime is infiltrating legitimate business activities and depriving honest businessmen of the right to make a living.

The general court further finds that because organized crime carries on its activities through layers of insulation and behind a wall of secrecy, government has been unsuccessful in curtailing and eliminating it. Normal investigative procedures are not effective in the investigation of illegal acts committed by organized crime. Therefore, law enforcement officials must be permitted to use modern methods of electronic surveillance, under strict judicial supervision, when investigating these organized criminal activities.

The general court further finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited. The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime.

B. Definitions. As used in this section--

1. The term "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.

2. The term "oral communication" means speech, except such speech as is transmitted over the public air waves by radio or other similar device.

3. The term "intercepting device" means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and other than any telephone or telegraph instrument, equipment, facility, or a component thereof, (a)

furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business.

4. The term "interception" means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication; provided that it shall not constitute an interception for an investigative or law enforcement officer, as defined in this section, to record or transmit a wire or oral communication if the officer is a party to such communication or has been given prior authorization to record or transmit the communication by such a party and if recorded or transmitted in the course of an investigation of a designated offense as defined herein.

5. The term "contents", when used with respect to any wire or oral communication, means any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication.

6. The term "aggrieved person" means any individual who was a party to an intercepted wire or oral communication or who was named in the warrant authorizing the interception, or who would otherwise have standing to complain that his personal or property interest or privacy was invaded in the course of an interception.

7. The term "designated offense" shall include the following offenses in connection with organized crime as defined in the preamble: arson, assault and battery with a dangerous weapon, extortion, bribery, burglary, embezzlement, forgery, gaming in violation of section seventeen of chapter two hundred and seventy-one of the general laws, intimidation of a witness or juror, kidnapping, larceny, lending of money or things of value in violation of the general laws, mayhem, murder, any offense involving the possession or sale of a narcotic or harmful drug, perjury, prostitution, robbery, subornation of perjury, any violation of this section, being an accessory to any of the foregoing offenses and conspiracy or attempt or solicitation to commit any of the foregoing offenses.

8. The term "investigative or law enforcement officer" means any officer of the United States, a state or a political subdivision of a state, who is empowered by law to conduct investigations of, or to make arrests for, the designated offenses, and any attorney authorized by law to participate in the prosecution of such offenses.

9. The term "judge of competent jurisdiction" means any justice of the superior court of the commonwealth.

10. The term "chief justice" means the chief justice of the superior court of the commonwealth.

11. The term "issuing judge" means any justice of the superior court who shall issue a warrant as provided herein or in the event of his disability or unavailability any other judge of competent jurisdiction designated by the chief justice.

12. The term "communication common carrier" means any person engaged as a common carrier in providing or operating wire communication facilities.

13. The term "person" means any individual, partnership, association, joint stock company, trust, or corporation, whether or not any of the foregoing is an officer, agent or employee of the United States, a state, or a political subdivision of a state.

14. The terms “sworn” or “under oath” as they appear in this section shall mean an oath or affirmation or a statement subscribed to under the pains and penalties of perjury.

15. The terms “applicant attorney general” or “applicant district attorney” shall mean the attorney general of the commonwealth or a district attorney of the commonwealth who has made application for a warrant pursuant to this section.

16. The term “exigent circumstances” shall mean the showing of special facts to the issuing judge as to the nature of the investigation for which a warrant is sought pursuant to this section which require secrecy in order to obtain the information desired from the interception sought to be authorized.

17. The term “financial institution” shall mean a bank, as defined in section 1 of chapter 167, and an investment bank, securities broker, securities dealer, investment adviser, mutual fund, investment company or securities custodian as defined in section 1.165-12(c)(1) of the United States Treasury regulations.

18. The term “corporate and institutional trading partners” shall mean financial institutions and general business entities and corporations which engage in the business of cash and asset management, asset management directed to custody operations, securities trading, and wholesale capital markets including foreign exchange, securities lending, and the purchase, sale or exchange of securities, options, futures, swaps, derivatives, repurchase agreements and other similar financial instruments with such financial institution.

C. Offenses.

1. Interception, oral communications prohibited.

Except as otherwise specifically provided in this section any person who--

willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment.

Proof of the installation of any intercepting device by any person under circumstances evincing an intent to commit an interception, which is not authorized or permitted by this section, shall be prima facie evidence of a violation of this subparagraph.

2. Editing of tape recordings in judicial proceeding prohibited.

Except as otherwise specifically provided in this section any person who willfully edits, alters or tampers with any tape, transcription or recording of oral or wire communications by any means, or attempts to edit, alter or tamper with any tape, transcription or recording of oral or wire communications by any means with the intent to present in any judicial proceeding or proceeding under oath, or who presents such recording or permits such recording to be presented in any judicial proceeding or proceeding under oath, without fully indicating the nature of the changes made in the original state of the recording, shall be

fined not more than ten thousand dollars or imprisoned in the state prison for not more than five years or imprisoned in a jail or house of correction for not more than two years or both so fined and given one such imprisonment.

3. Disclosure or use of wire or oral communications prohibited.

Except as otherwise specifically provided in this section any person who--

a. willfully discloses or attempts to disclose to any person the contents of any wire or oral communication, knowing that the information was obtained through interception; or

b. willfully uses or attempts to use the contents of any wire or oral communication, knowing that the information was obtained through interception, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

4. Disclosure of contents of applications, warrants, renewals, and returns prohibited.

Except as otherwise specifically provided in this section any person who--

willfully discloses to any person, any information concerning or contained in, the application for, the granting or denial of orders for interception, renewals, notice or return on an ex parte order granted pursuant to this section, or the contents of any document, tape, or recording kept in accordance with paragraph N, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

5. Possession of interception devices prohibited.

A person who possesses any intercepting device under circumstances evincing an intent to commit an interception not permitted or authorized by this section, or a person who permits an intercepting device to be used or employed for an interception not permitted or authorized by this section, or a person who possesses an intercepting device knowing that the same is intended to be used to commit an interception not permitted or authorized by this section, shall be guilty of a misdemeanor punishable by imprisonment in a jail or house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

The installation of any such intercepting device by such person or with his permission or at his direction shall be prima facie evidence of possession as required by this subparagraph.

6. Any person who permits or on behalf of any other person commits or attempts to commit, or any person who participates in a conspiracy to commit or to attempt to commit, or any accessory to a person who commits a violation of subparagraphs 1 through 5 of paragraph C of this section shall be punished in the same manner as is provided for the respective offenses as described in subparagraphs 1 through 5 of paragraph C.

D. Exemptions.

1. Permitted interception of wire or oral communications.

It shall not be a violation of this section--

- a. for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of such communication, or which is necessary to prevent the use of such facilities in violation of section fourteen A of chapter two hundred and sixty-nine of the general laws; provided, that said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.
- b. for persons to possess an office intercommunication system which is used in the ordinary course of their business or to use such office intercommunication system in the ordinary course of their business.
- c. for investigative and law enforcement officers of the United States of America to violate the provisions of this section if acting pursuant to authority of the laws of the United States and within the scope of their authority.
- d. for any person duly authorized to make specified interceptions by a warrant issued pursuant to this section.
- e. for investigative or law enforcement officers to violate the provisions of this section for the purposes of ensuring the safety of any law enforcement officer or agent thereof who is acting in an undercover capacity, or as a witness for the commonwealth; provided, however, that any such interception which is not otherwise permitted by this section shall be deemed unlawful for purposes of paragraph P.
- f. for a financial institution to record telephone communications with its corporate or institutional trading partners in the ordinary course of its business; provided, however, that such financial institution shall establish and maintain a procedure to provide semi-annual written notice to its corporate and institutional trading partners that telephone communications over designated lines will be recorded.

2. Permitted disclosure and use of intercepted wire or oral communications.

- a. Any investigative or law enforcement officer, who, by any means authorized by this section, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents or evidence in the proper performance of his official duties.
- b. Any investigative or law enforcement officer, who, by any means authorized by this section has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may use such contents or evidence in the proper performance of his official duties.
- c. Any person who has obtained, by any means authorized by this section, knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents while giving testimony under oath or affirmation in any criminal proceeding in any court of the United States or of any state or in any federal or state grand jury proceeding.

d. The contents of any wire or oral communication intercepted pursuant to a warrant in accordance with the provisions of this section, or evidence derived therefrom, may otherwise be disclosed only upon a showing of good cause before a judge of competent jurisdiction.

e. No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this section shall lose its privileged character.

E. Warrants: when issuable:

A warrant may issue only:

1. Upon a sworn application in conformity with this section; and
2. Upon a showing by the applicant that there is probable cause to believe that a designated offense has been, is being, or is about to be committed and that evidence of the commission of such an offense may thus be obtained or that information which will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense may thus be obtained; and
3. Upon a showing by the applicant that normal investigative procedures have been tried and have failed or reasonably appear unlikely to succeed if tried.

F. Warrants: application.

1. Application. The attorney general, any assistant attorney general specially designated by the attorney general, any district attorney, or any assistant district attorney specially designated by the district attorney may apply ex parte to a judge of competent jurisdiction for a warrant to intercept wire or oral communications. Each application ex parte for a warrant must be in writing, subscribed and sworn to by the applicant authorized by this subparagraph.

2. The application must contain the following:

- a. A statement of facts establishing probable cause to believe that a particularly described designated offense has been, is being, or is about to be committed; and
- b. A statement of facts establishing probable cause to believe that oral or wire communications of a particularly described person will constitute evidence of such designated offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense; and
- c. That the oral or wire communications of the particularly described person or persons will occur in a particularly described place and premises or over particularly described telephone or telegraph lines; and

- d. A particular description of the nature of the oral or wire communications sought to be overheard; and
- e. A statement that the oral or wire communications sought are material to a particularly described investigation or prosecution and that such conversations are not legally privileged; and
- f. A statement of the period of time for which the interception is required to be maintained. If practicable, the application should designate hours of the day or night during which the oral or wire communications may be reasonably expected to occur. If the nature of the investigation is such that the authorization for the interception should not automatically terminate when the described oral or wire communications have been first obtained, the application must specifically state facts establishing probable cause to believe that additional oral or wire communications of the same nature will occur thereafter; and
- g. If it is reasonably necessary to make a secret entry upon a private place and premises in order to install an intercepting device to effectuate the interception, a statement to such effect; and
- h. If a prior application has been submitted or a warrant previously obtained for interception of oral or wire communications, a statement fully disclosing the date, court, applicant, execution, results, and present status thereof; and
- i. If there is good cause for requiring the postponement of service pursuant to paragraph L, subparagraph 2, a description of such circumstances, including reasons for the applicant's belief that secrecy is essential to obtaining the evidence or information sought.

3. Allegations of fact in the application may be based either upon the personal knowledge of the applicant or upon information and belief. If the applicant personally knows the facts alleged, it must be so stated. If the facts establishing such probable cause are derived in whole or part from the statements of persons other than the applicant, the sources of such information and belief must be either disclosed or described; and the application must contain facts establishing the existence and reliability of any informant and the reliability of the information supplied by him. The application must also state, so far as possible, the basis of the informant's knowledge or belief. If the applicant's information and belief is derived from tangible evidence or recorded oral evidence, a copy or detailed description thereof should be annexed to or included in the application. Affidavits of persons other than the applicant may be submitted in conjunction with the application if they tend to support any fact or conclusion alleged therein. Such accompanying affidavits may be based either on personal knowledge of the affiant or information and belief, with the source thereof, and reason therefor, specified.

G. Warrants: application to whom made.

Application for a warrant authorized by this section must be made to a judge of competent jurisdiction in the county where the interception is to occur, or the county where the office of the applicant is located, or in the event that there is no judge of competent jurisdiction sitting in said county at such time, to a judge of competent jurisdiction sitting in Suffolk County; except that for these purposes, the office of the attorney general shall be deemed to be located in Suffolk County.

H. Warrants: application how determined.

1. If the application conforms to paragraph F, the issuing judge may examine under oath any person for the purpose of determining whether probable cause exists for the issuance of the warrant pursuant to paragraph E. A verbatim transcript of every such interrogation or examination must be taken, and a transcription of the same, sworn to by the stenographer, shall be attached to the application and be deemed a part thereof.

2. If satisfied that probable cause exists for the issuance of a warrant the judge may grant the application and issue a warrant in accordance with paragraph I. The application and an attested copy of the warrant shall be retained by the issuing judge and transported to the chief justice of the superior court in accordance with the provisions of paragraph N of this section.

3. If the application does not conform to paragraph F, or if the judge is not satisfied that probable cause has been shown sufficient for the issuance of a warrant, the application must be denied.

I. Warrants: form and content.

A warrant must contain the following:

1. The subscription and title of the issuing judge; and

2. The date of issuance, the date of effect, and termination date which in no event shall exceed thirty days from the date of effect. The warrant shall permit interception of oral or wire communications for a period not to exceed fifteen days. If physical installation of a device is necessary, the thirty-day period shall begin upon the date of installation. If the effective period of the warrant is to terminate upon the acquisition of particular evidence or information or oral or wire communication, the warrant shall so provide; and

3. A particular description of the person and the place, premises or telephone or telegraph line upon which the interception may be conducted; and

4. A particular description of the nature of the oral or wire communications to be obtained by the interception including a statement of the designated offense to which they relate; and

5. An express authorization to make secret entry upon a private place or premises to install a specified intercepting device, if such entry is necessary to execute the warrant; and

6. A statement providing for service of the warrant pursuant to paragraph L except that if there has been a finding of good cause shown requiring the postponement of such service, a statement of such finding together with the basis therefor must be included and an alternative direction for deferred service pursuant to paragraph L, subparagraph 2.

J. Warrants: renewals.

1. Any time prior to the expiration of a warrant or a renewal thereof, the applicant may apply to the issuing judge for a renewal thereof with respect to the same person, place, premises or telephone or telegraph line. An application for renewal

must incorporate the warrant sought to be renewed together with the application therefor and any accompanying papers upon which it was issued. The application for renewal must set forth the results of the interceptions thus far conducted. In addition, it must set forth present grounds for extension in conformity with paragraph F, and the judge may interrogate under oath and in such an event a transcript must be provided and attached to the renewal application in the same manner as is set forth in subparagraph 1 of paragraph H.

2. Upon such application, the judge may issue an order renewing the warrant and extending the authorization for a period not exceeding fifteen (15) days from the entry thereof. Such an order shall specify the grounds for the issuance thereof. The application and an attested copy of the order shall be retained by the issuing judge to be transported to the chief justice in accordance with the provisions of subparagraph N of this section. In no event shall a renewal be granted which shall terminate later than two years following the effective date of the warrant.

K. Warrants: manner and time of execution.

1. A warrant may be executed pursuant to its terms anywhere in the commonwealth.

2. Such warrant may be executed by the authorized applicant personally or by any investigative or law enforcement officer of the commonwealth designated by him for the purpose.

3. The warrant may be executed according to its terms during the hours specified therein, and for the period therein authorized, or a part thereof. The authorization shall terminate upon the acquisition of the oral or wire communications, evidence or information described in the warrant. Upon termination of the authorization in the warrant and any renewals thereof, the interception must cease at once, and any device installed for the purpose of the interception must be removed as soon thereafter as practicable. Entry upon private premises for the removal of such device is deemed to be authorized by the warrant.

L. Warrants: service thereof.

1. Prior to the execution of a warrant authorized by this section or any renewal thereof, an attested copy of the warrant or the renewal must, except as otherwise provided in subparagraph 2 of this paragraph, be served upon a person whose oral or wire communications are to be obtained, and if an intercepting device is to be installed, upon the owner, lessee, or occupant of the place or premises, or upon the subscriber to the telephone or owner or lessee of the telegraph line described in the warrant.

2. If the application specially alleges exigent circumstances requiring the postponement of service and the issuing judge finds that such circumstances exist, the warrant may provide that an attested copy thereof may be served within thirty days after the expiration of the warrant or, in case of any renewals thereof, within thirty days after the expiration of the last renewal; except that upon a showing of important special facts which set forth the need for continued secrecy to the satisfaction of the issuing judge, said judge may direct that the attested copy of the warrant be served on such parties as are required by this section at such time as may be appropriate in the circumstances but in no event may he order it to be served later than three (3) years from the time of expiration of the warrant or the last renewal thereof. In the event that the service required herein is postponed in accordance with this paragraph, in addition to the requirements of any other paragraph of this section, service of an attested copy of the warrant shall be made upon any aggrieved person who should reasonably be known to the person who executed or obtained the warrant as a result of the information obtained from the interception authorized thereby.

3. The attested copy of the warrant shall be served on persons required by this section by an investigative or law enforcement officer of the commonwealth by leaving the same at his usual place of abode, or in hand, or if this is not possible by mailing the same by certified or registered mail to his last known place of abode. A return of service shall be made to the issuing judge, except, that if such service is postponed as provided in subparagraph 2 of paragraph L, it shall be made to the chief justice. The return of service shall be deemed a part of the return of the warrant and attached thereto.

M. Warrant: return.

Within seven days after termination of the warrant or the last renewal thereof, a return must be made thereon to the judge issuing the warrant by the applicant therefor, containing the following:

- a. a statement of the nature and location of the communications facilities, if any, and premise or places where the interceptions were made; and
- b. the periods of time during which such interceptions were made; and
- c. the names of the parties to the communications intercepted if known; and
- d. the original recording of the oral or wire communications intercepted, if any; and
- e. a statement attested under the pains and penalties of perjury by each person who heard oral or wire communications as a result of the interception authorized by the warrant, which were not recorded, stating everything that was overheard to the best of his recollection at the time of the execution of the statement.

N. Custody and secrecy of papers and recordings made pursuant to a warrant.

1. The contents of any wire or oral communication intercepted pursuant to a warrant issued pursuant to this section shall, if possible, be recorded on tape or wire or other similar device. Duplicate recordings may be made for use pursuant to subparagraphs 2 (a) and (b) of paragraph D for investigations. Upon examination of the return and a determination that it complies with this section, the issuing judge shall forthwith order that the application, all renewal applications, warrant, all renewal orders and the return thereto be transmitted to the chief justice by such persons as he shall designate. Their contents shall not be disclosed except as provided in this section. The application, renewal applications, warrant, the renewal order and the return or any one of them or any part of them may be transferred to any trial court, grand jury proceeding of any jurisdiction by any law enforcement or investigative officer or court officer designated by the chief justice and a trial justice may allow them to be disclosed in accordance with paragraph D, subparagraph 2, or paragraph O or any other applicable provision of this section.

The application, all renewal applications, warrant, all renewal orders and the return shall be stored in a secure place which shall be designated by the chief justice, to which access shall be denied to all persons except the chief justice or such court officers or administrative personnel of the court as he shall designate.

2. Any violation of the terms and conditions of any order of the chief justice, pursuant to the authority granted in this paragraph, shall be punished as a criminal contempt of court in addition to any other punishment authorized by law.

3. The application, warrant, renewal and return shall be kept for a period of five (5) years from the date of the issuance of the warrant or the last renewal thereof at which time they shall be destroyed by a person designated by the chief justice. Notice prior to the destruction shall be given to the applicant attorney general or his successor or the applicant district attorney or his successor and upon a showing of good cause to the chief justice, the application, warrant, renewal, and return may be kept for such additional period as the chief justice shall determine but in no event longer than the longest period of limitation for any designated offense specified in the warrant, after which time they must be destroyed by a person designated by the chief justice.

O. Introduction of evidence.

1. Notwithstanding any other provisions of this section or any order issued pursuant thereto, in any criminal trial where the commonwealth intends to offer in evidence any portions of the contents of any interception or any evidence derived therefrom the defendant shall be served with a complete copy of each document and item which make up each application, renewal application, warrant, renewal order, and return pursuant to which the information was obtained, except that he shall be furnished a copy of any recording instead of the original. The service must be made at the arraignment of the defendant or, if a period in excess of thirty (30) days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty (30) days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed, at least thirty days before the commencement of the criminal trial, shall render such evidence illegally obtained for purposes of the trial against the defendant; and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court.

2. In any criminal trial where the commonwealth intends to offer in evidence any portions of a recording or transmission or any evidence derived therefrom, made pursuant to the exceptions set forth in paragraph B, subparagraph 4, of this section, the defendant shall be served with a complete copy of each recording or a statement under oath of the evidence overheard as a result of the transmission. The service must be made at the arraignment of the defendant or if a period in excess of thirty days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed at least thirty days before the commencement of the criminal trial, shall render such service illegally obtained for purposes of the trial against the defendant and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court.

P. Suppression of evidence.

Any person who is a defendant in a criminal trial in a court of the commonwealth may move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom, for the following reasons:

1. That the communication was unlawfully intercepted.

2. That the communication was not intercepted in accordance with the terms of this section.
3. That the application or renewal application fails to set forth facts sufficient to establish probable cause for the issuance of a warrant.
4. That the interception was not made in conformity with the warrant.
5. That the evidence sought to be introduced was illegally obtained.
6. That the warrant does not conform to the provisions of this section.

Q. Civil remedy.

Any aggrieved person whose oral or wire communications were intercepted, disclosed or used except as permitted or authorized by this section or whose personal or property interests or privacy were violated by means of an interception except as permitted or authorized by this section shall have a civil cause of action against any person who so intercepts, discloses or uses such communications or who so violates his personal, property or privacy interest, 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 per day for each day of violation or \$1000, whichever is higher;
2. punitive damages; and
3. a reasonable attorney's fee and other litigation disbursements reasonably incurred. Good faith reliance on a warrant issued under this section shall constitute a complete defense to an action brought under this paragraph.

R. Annual report of interceptions of the general court.

On the second Friday of January, each year, the attorney general and each district attorney shall submit a report to the general court stating (1) the number of applications made for warrants during the previous year, (2) the name of the applicant, (3) the number of warrants issued, (4) the effective period for the warrants, (5) the number and designation of the offenses for which those applications were sought, and for each of the designated offenses the following: (a) the number of renewals, (b) the number of interceptions made during the previous year, (c) the number of indictments believed to be obtained as a result of those interceptions, (d) the number of criminal convictions obtained in trials where interception evidence or evidence derived therefrom was introduced. This report shall be a public document and be made available to the public at the offices of the attorney general and district attorneys. In the event of failure to comply with the provisions of this paragraph any person may compel compliance by means of an action of mandamus.

Credits

Amended by St.1959, c. 449, § 1; St.1968, c. 738, § 1; St.1986, c. 557, § 199; St.1993, c. 432, § 13; St.1998, c. 163, §§ 7, 8.

§ 99. Interception of wire and oral communications, MA ST 272 § 99

Notes of Decisions (304)

M.G.L.A. 272 § 99, MA ST 272 § 99

Current through Chapter 84 of the 2015 1st Annual Session

End of Document

© 2015 Thomson Reuters. No claim to original U.S. Government Works.

IMPOUNDED

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

**SUPERIOR COURT
CIVIL ACTION
No. 11-2808-BLS1**

DEBORAH L. MARQUIS

vs.

GOOGLE, INC.

**MEMORANDUM AND ORDER ON
CROSS-MOTIONS FOR SUMMARY JUDGMENT**

This action tests whether Google, in its automated scanning of emails sent between Gmail accounts and non-Gmail accounts – in significant part to facilitate targeted or personalized advertising directed at Gmail users – violates Massachusetts’ wiretap statute, G.L. c. 272, §99. Because I conclude that the statute does not apply to the extraterritorial conduct at issue, Google’s motion to dismiss the complaint is allowed.

FACTS

The following facts are not subject to genuine dispute. Gmail is a web-based email service that Google provides without charge to more than 69 million Americans and hundreds of millions worldwide. The plaintiff uses an AOL email platform, but she sends and receives emails to and from Gmail accounts.¹

¹The case was filed as a class action. On June 19, 2014, the Court (Kaplan, J.) denied the motion for class certification, “except with respect to a possible class of non-Gmail email users that exchanged emails with an email user whose email service was provided by a Google Apps customer who permitted targeted advertising; and as to such a possible class, the court [made] no ruling.” The issue has not been pursued further.

From the time that Gmail was launched in 2004, Google has used automated technologies to scan emails received by Gmail users and, at times, emails sent from Gmail accounts. These enable Google to provide “targeted” or “personalized” advertising (for the difference, see below) to Gmail users. This generates revenue for Google, at least some of which goes to offset the cost of providing Gmail for free.² Scanning emails also facilitates services unrelated to advertising that reduce cost, increase efficiency, and enhance the user experience. These include detection and interruption of spam, viruses and “phishing” emails; implementation of user-created filters; automated categorization of emails; enabling the user to search within the account for keywords; identifying dates to facilitate reminders on the user’s Google calendar; and identifying shipping notifications so that the user may click a button to fetch package tracking information.

Google’s methods of scanning emails, then using the results to select targeted or personalized advertising, have evolved with the passage of time. Until [REDACTED] – and since then to the present day, but to a much lesser extent – Google has used what will be referred to herein as the [REDACTED] process. Once an incoming email has been [REDACTED]

[REDACTED]³ The results are then forwarded to a [REDACTED] server which

²The other major email platforms also use some form of targeted advertising. The largest in the U.S. – Yahoo! – informs its users that it provides personally relevant features, content and advertising by scanning and analyzing the content of Mail!, Messenger, and other communications. Microsoft and AOL have also publicized the fact that they target advertising using, in part, information gleaned from use of their sites; this includes users’ search patterns and other data but not, apparently, message content.

³These three requirements – [REDACTED] – mean that not all emails sent to Gmail accounts were (or are) scanned. Roughly [REDACTED]

processes the information, looking for keywords that are then used in selecting advertisements to be displayed to the user as he or she views the email.

Google's term for this is "targeted advertising." In specific circumstances, Google also scans outgoing emails, then directs the Gmail user to the Inbox where an ad based on the just-sent email is displayed.

[REDACTED] processing is automated and does not involve human review. Neither the sender nor the recipient of an email involving a Gmail account is notified that Google has scanned it.

In or about [REDACTED] Google implemented a new system called "User Modeling" or "Personalized Advertising." User Modeling has largely but not entirely supplanted the [REDACTED] system, which remains in limited use. A server using Google's Content Onebox ("COB") technology scans the text of emails sent to a Gmail user for keywords and other information that can be used to select advertising likely to be relevant to the Gmail user's interests.⁴ [REDACTED]

[REDACTED] At times, the system has then added to the incoming email's metadata stored on Google servers, but not to the message

[REDACTED]

[REDACTED] Many of these exceptions are beyond the control of the email's sender, and none are particularly germane to the legal issues presented here.

⁴As with the [REDACTED]

[REDACTED]

sent to the user, [REDACTED]

A "User Model Server" uses the information gathered from COB scanning as well as other factors to construct the Gmail user's "User Model." This is based on the user's most recent emails.

Most information in a User Model [REDACTED]

[REDACTED] User Modeling is used to select for Gmail users what Google calls "personalized advertising," selected to correspond with what the User Model suggests are the user's interests. As with [REDACTED] all of this is done through a series of automated steps on large servers, not human review.⁵

All of the scanning processes that implement targeted or personalized advertising are implemented on servers located outside of Massachusetts. The code that implements the [REDACTED]

[REDACTED] The code that implements the User Model process is run [REDACTED]

None of the processing occurs in Massachusetts.

⁵A Gmail user may opt out of personalized advertising. In that case, a COB server will [REDACTED]

Google's "Create and Account" page (see below) does not require or permit an account holder to provide his or her state of residence. Nor is there any reliable way for Google to determine the residence of a non-Gmail user who sends an email to, or receives one from, a Gmail account.⁶

Although Google is highly protective of its proprietary information concerning scanning protocols – hence, the likelihood that the publicly released version of this decision will contain some redactions – the fact that it scans emails and uses the results to correlate advertising with subscribers' interests has been widely publicized, to Gmail users and others. Since at least 2008⁷ the "Create An Account" page by which users sign up for Gmail has explained,

With Gmail, you won't see blinking banner ads. Instead, we display ads you might find useful that are relevant to the content of your emails.

This is immediately followed by a link by which the would-be subscriber is invited to "[Learn more](#)" by viewing a page titled "Ads in Gmail and your personal data." This begins:

⁶A Google witness was questioned at some length whether an incoming email came with the sender's IP address as metadata; if so, whether this would enable to determine the physical location of the internet connection from which the email was sent; and if so, how accurately. The didn't know the answer to any of these questions, on which the record is otherwise silent, and neither do I. The plaintiff's response – that perhaps voter lists would be of assistance – may have been germane to the question of class certification, but it has little relevance to the issue at hand. Although I take judicial notice of the fact that police officers have been able to subpoena account information from the internet service provider that supplied a known IP address, this is not to say that Google could do this in real time, or without a subpoena. Finally, Gmail is a web-based platform that may be accessed from any computer or mobile device; even knowing the precise physical address from which an email was sent is not the same thing as knowing the sender's state of residence.

⁷Google's disclosures, like the technology and its use, have evolved over time. Current versions are available to all on line, and prior versions of some are similarly available on "archive" pages.

How Gmail Ads Work

Ads that appear next to Gmail messages are similar to ads that appear next to Google search results and on content pages throughout the web. In Gmail, ads are related to the content of your messages. Our goal is to provide Gmail users with ads that are useful and relevant to their interests.

Ad targeting in Gmail is fully automated, and no humans read your email in order to target advertisements or related information. This type of automated scanning is how many email services, not just Gmail, provide features like spam filtering and spell checking. Ads are selected for relevance and served by Google computers using the same contextual advertising technology that powers Google's [AdSense program](#) [another link].

Google's Terms of Service and Privacy Policies – to which all subscribers must acknowledge and agree when creating a Gmail account – also disclose in general fashion that Google collects data from users, and specify that Google will use data only to provide its services, develop new services, and for security reasons. For example, the Terms of Service document in place from April 2007 until March 2012 stated:

Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.

Services are defined as, "Google's products, software, services and web sites." Since March 2012, the successor document has said,

Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies.

The current Google Privacy Policy advises users that Google collects information regarding how they use Google services, and that it “use[s] this information to offer you tailored content – like giving you more relevant search results and ads.”

From at least October 14, 2005 to October 3, 2010, Google also maintained a separate Gmail Privacy Policy, which disclosed explicitly that Google processes emails in order to provide various features of Gmail. For example, a link to a “Gmail Privacy Notice” from the navigation bar in the Google Privacy Policy dated October 14, 2005 advised,

Google maintains and processes your Gmail account and its contents to provide the Gmail service to you and to improve our services. The Gmail service includes relevant advertising and related links based on the IP address, *content of messages* and other information related to your use of Gmail. Google’s computers process the information in your messages for various purposes, including formatting and displaying the information to you, delivering advertisements and related links, preventing unsolicited bulk email (spam), backing up your messages, and other purposes relating to offering you Gmail. (Emphasis supplied.)

Google’s website has “Help” pages and Google tools that allow users to customize their privacy and advertising settings. The language of the Help pages has changed over time. One is the “Ads in Gmail and your personal data” page linked to the “Create and Account page and quoted above. This Help page received over [REDACTED] views from 2010 to 2012.

From December of 2011 to December of 2012, another Help page had the following:

Is Google reading my mail?

No, but automatic scanning and filtering technology is at the heart of Gmail. Gmail scans and processes all messages using fully automated systems in order to do useful and innovative stuff like filter spam, detect viruses and malware, show relevant ads, and develop and deliver new features across your Google experience. Priority Inbox, spell checking, forwarding, auto-responding,

automatic saving and sorting, and converting URLs to clickable links are just a few of the many features that use this kind of automatic processing.

All of this information, of course, is directed at Gmail users. Although Google's Terms of Use or Privacy Policies are readily available on line, they are not explicitly directed at non-Gmail users.

Since the 2004 launch, however, numerous major and not-so-major media outlets have reported extensively – some favorably, some not – on Gmail's automated scanning feature and its use in facilitating targeted or personalized advertising.⁸ An email recipient or sender who had encountered the media coverage, and noticed that the correspondent's email address ended in ".gmail," might make the connection, or might not. In fact the plaintiff, a resident of Boxford, Massachusetts with an AOL email account, did not realize that her emails to Gmail accounts were being scanned until shortly before her complaint was filed on July 29, 2011.

Even a sender who knows that Google scans emails sent to and from a Gmail account, moreover, may not know that a particular correspondent is using Gmail, because not all Gmail accounts have "@gmail" addresses. Google Apps, a suite of productivity and collaboration tools and software – including a version of Gmail – is offered on a subscription basis to businesses,

⁸Judge Kaplan's class certification decision summarizes facts concerning media coverage found in a declaration of Kyle Wong dated January 17, 2014, which was submitted with the certification motion papers but not with the summary judgment papers. See Memorandum of Decision and Order on Plaintiff's Motion for Class Certification (Papers #48, #49; Kaplan, J.), pp. 6-8.

Of particular interest locally is a column by Hiawatha Bray in the May 31, 2004 Boston Globe titled, "Google's Gmail Is Still a Rough Draft." In Bray's estimation, "Google's plan to make money off the [Gmail] service by featuring ads inspired by the contents of the e-mail messages" was "[n]ot really" intrusive; "Indeed, it's sort of cool. ... Unlike most ads, these relate to something that interests you, so you'll almost certainly read them."

educational organizations, and internet service providers, and allows subscribers to use their own domain name (e.g., @yourcompany.com, @yourcollege.edu, etc.). Someone corresponding with an employee at a company or institution that subscribes to Google Apps, therefore, would not know from the email address that this is a Gmail account.⁹

In short: regardless of Google's disclosures to its Gmail accountholders and general knowledge derived from press accounts, one may not assume that all of those with whom those accountholders correspond by email—including, before July 2011, the plaintiff—are aware that some of the correspondence will likely be subject to an automated scanning process.

DISCUSSION

A. **The Massachusetts Wiretap Statute.**

The Massachusetts wiretap statute, G.L. c. 272, §99, has its antecedents in Chapter 558 of the Statutes of 1920. It substantially rewritten in 1959 and again in 1968. Since then, there have been only minor and, for present purposes, irrelevant revisions in 1986, 1993, and 1998, described in the margin.¹⁰ For present purposes, therefore, the statute is effectively 46 years old, and has

⁹Google Apps' email function has other features that differentiate it from a stand-alone Gmail subscription. For example, the system administrator of the entity subscribing to Google Apps determines the content and implementation of terms of service, use policies, or privacy policies associated with end user accounts, including whether and how the user may opt in or out of advertising.

¹⁰The 1986 amendment was purely technical, removing the redundant figure "\$10,000" in subpart C.2's imposition of a criminal fine of ten thousand dollars for tampering with the transcript of a judicial proceeding. In 1993, subpart D.1.e was added, permitting law enforcement officer and agents to wear wires to ensure their safety; the amendment also specified that "the law in effect at the time an offense is committed shall govern sentencing for such offense." The 1998 amendment, by adding subparts B.17, B.18, and D.1.f, added "ordinary course of business" exemptions specific to the financial industry.

remained materially unchanged since well before the advent of personal computers, the Internet, internet advertising, and web-based email.

The statute as now written provides that

any person who ... willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment.

G.L. c. 272, §99.C.1.¹¹ Subsection Q additionally provides for civil remedies for an unlawful interception, including actual damages or liquidated damages in the higher amount of \$100 per day of violation or \$1000, punitive damages, and attorneys' fees and costs. The statute does not distinguish between conduct that is punishable criminally and that which is subject to civil remedies; an act either is an unlawful interception, or it isn't.

Central to the statute is the definition of "interception," which contains a "one-party consent" exception for law enforcement officials investigating certain "designated offenses" enumerated elsewhere in the statute:

The term "interception" means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication; provided that it shall not constitute an interception for an investigative or law enforcement officer, as defined in this section, to record or transmit a wire or oral communication if the officer is a party to such communication or has been given prior authorization to record or transmit the communication by such a party

¹¹Additional offenses under the statute include disclosure or use of unlawfully intercepted communications, possession of an interception device, and aiding and abetting an unlawful interception. G.L. c. 272, §99.C.2-6.

and if recorded or transmitted in the course of an investigation of a designated offense as defined herein. (G.L. 272, §99.B.4.)

An exemption at G.L. c. 272, §99.D.1.d additionally allows law enforcement to engage in non-consensual interceptions authorized by a warrant.

Massachusetts' is thus, at least where civilians are concerned, a two-party consent law, in that consent to an otherwise prohibited interception must be given by "all parties to [the] communication." This distinguishes the Massachusetts law from the federal Electronic Communications Privacy Act of 1986 (ECPA), Pub.L. 99-508, 100 Stat. 1848 (1986), (codified at 18 U.S.C. §2511 and elsewhere)¹² and most state wiretap statutes,¹³ which permit interceptions with the consent of just one party.

Several of the other statutory definitions and the exceptions embedded therein are potentially germane to this case. They include the following:

The term "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception. (G.L. 272, §99.B.1.)

¹²The ECPA permits interceptions by a civilian party "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 unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. §2511(2)(d) (emphasis supplied).

¹³Thirty-eight states plus the District of Columbia have one-party consent laws, while eleven – California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania and Washington – have various sorts of two-party consent statutes. See Digital Media Law Project, "Recording Phone Calls and Conversations," available at: <http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations>. The Illinois statute was recently ruled unconstitutionally overbroad and violative of the First Amendment. People v. Melongo, 2014 IL 114852, 379 Ill. Dec. 43, 6 N.E.3d 120 (Ill. Supr. 2014).

The term "intercepting device" means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and *other than* any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business. (G.L. 272, §99.B.3; emphasis supplied)

The term "communication common carrier" means any person engaged as a common carrier in providing or operating wire communication facilities. (G.L. 272, §99.B.12.)

The parties appear to agree that because the internet depends on cable connections, emails constitute "wire communications." Google argues, however, (1) that the "ordinary course of business" exception to the statutory definition of an "intercepting device" (G.L. 272, §99.B.3) applies to both [REDACTED] and the User Model process; (2) that [REDACTED] is additionally exempted because scanning emails after they reach the recipient is not an "interception" within the meaning of (G.L. 272, §99.B.4); (3) that the scanning, having taken place outside of Massachusetts, is not subject to the Massachusetts wiretap statute in any event; and (4) that if all else fails, the plaintiff is at least barred from claiming relief for scanning that occurred after she became aware of the practice.

Because I conclude that the statute does not apply to an interception occurring outside Massachusetts, it is unnecessary to reach the other issues Google has raised, other than to note that each raises interesting and, at times, challenging issues of statutory construction. These are

especially apparent in the “ordinary course of business” defense and emanate in part – but only in part – from the fact that unlike the federal ECPA, the Massachusetts statute has remained fundamentally unchanged since 1986, and so has occasionally undergone awkward but necessary judicial updating to “maintain its viability in the broad run of cases” while keeping pace with changes in technology and commerce. Commonwealth v. Moody, 466 Mass. 196, 207 (2013), quoting Dillon v. Massachusetts Bay Transp. Auth., 49 Mass. App. Ct. 309, 314-16 (2000).

B. Extraterritorial Application of the Massachusetts Wiretap Statute.

As noted above, the servers on which Google scans emails of Gmail users are physically located in [REDACTED]¹⁴ None are located in Massachusetts, and so no interceptions physically occur within our borders.

In a series of criminal and civil cases, Massachusetts and federal courts have declined to apply the Massachusetts wiretap statute to interceptions occurring outside Massachusetts. The sole appellate precedent on the issue is Commonwealth v. Wilcox, 63 Mass. App. Ct. 131, 139 (2005). There, the defendant gave a statement in a Rhode Island police station that the interrogating officer recorded without his knowledge. The Appeals Court upheld the trial court’s denial of a motion to suppress the statement, noting that “[t]he defendant cites no authority for the proposition that G.L.

¹⁴It may not be coincidental that these are all one-party consent jurisdictions (see footnote 13, *supra*). Nonetheless, at least one court has, in ruling on a motion to dismiss, found that Gmail users’ acceptance of Google’s Terms of Service and Privacy Policies “does not establish explicit consent” even on the part of Gmail account holders, because these documents are insufficiently explicit as to what Google does and how it uses the information thus obtained. In re: Google, Inc. Gmail Litigation, 2013 WL 5423918 (U.S. Dist. Ct., N.D. Cal., Sept. 26, 2013) at *12-*15. One might debate the point, but the federal court’s further holding “that non-Gmail users who are not subject to Google’s Privacy Policies or Terms of Service have [not] impliedly consented to Google’s interception of their emails to Gmail users” (*id.* at *14) seems all but irrefutable. Google has not advanced a consent argument in this case.

c. 272, § 99, applies to recordings made outside of Massachusetts.” Similarly, in Commonwealth v. Tibbs, 2007 WL 4644818 (Mass. Super. 2008; Gants, J.), a judge then of this Court, citing Wilcox, ruled admissible statements made in a Rhode Island jail by the defendant to a detainee secretly wearing a wire.

Closer to the present case on its facts, in that it concerned an interstate wire communication originating in Massachusetts and intercepted elsewhere, is Commonwealth v. Maccini, 2007 WL 1203560 (Mass. Super. 2007; Fabricant, J.). There, the defendant sent emails and instant messages from Massachusetts to a person who, unbeknownst to the sender, was the Chief of Police of the New Waterford, Ohio, Police Department, and was conducting an undercover investigation into trading of child pornography on the internet. The Chief saved the communications, which were then used in a Massachusetts investigation to obtain warrants to search the defendant’s AOL account and his computers. Holding that the Massachusetts wiretap statute did not apply, the court remarked:

A fundamental characteristic of the federal system is that each state is entitled to its own laws, subject to the supremacy of federal law, but that no state may impose its laws on another. See generally, Commonwealth v. Aarhus, 387 Mass. 735, 742 (1982). Massachusetts has not purported to do so; nothing in the wiretap statute suggests any intention to regulate conduct outside the bounds of the Commonwealth. See Commonwealth v. Wilcox, 63 Mass. App. Ct. 131, 139 (2005). Federal law permits recording with the consent of one party to the communication. See Commonwealth v. Blood, [400 Mass. 61, 67 (1987)], citing United States v. Caceres, 440 U.S. 741, 750-751 (1979), and United States v. White, 401 U.S. 745, 751 (1971). The defendant has identified no Ohio statute or other authority that would prohibit [Chief] Haueter’s conduct, and at argument conceded that none exists. Thus, Haueter’s conduct violated no law, and was not “unlawful” within the meaning of c. 272, §99P1. For that reason alone, the defendant’s motion to suppress must be denied.

Id. at *2.

At least two federal cases have reached the same conclusion in civil cases brought under the Massachusetts statute. In MacNeil Engineering Co. v. Trisport, Ltd., 59 F. Supp. 2d 199, 202 (D. Mass. 1999; Young, J.), the defendant recorded in England a telephone call originating in Massachusetts. And in Pendell v. AMS/Oil, Inc., 1986 WL 5286 (D. Mass. 1986; Collings, U.S.M.J.) at *4, the reverse occurred: a Rhode Island caller recorded his telephone call to a Massachusetts recipient. In both cases, the holding was that the Massachusetts statute did not apply to the out-of-state interception.

On the other hand, at least one decision from this Court, noting the lack of binding precedent and applying principles drawn from the Restatement (Second) of Conflict of Laws, has applied the statute to an interstate telephone call emanating in Massachusetts and recorded by the recipient in Virginia. Heffernan v. Hashampour, 2009 WL 6361870 (Mass. Super. 2009). The facts in the present case, however, underscore the wisdom of the Maccini, MacNeil Engineering and Pendell holdings, particularly when one leaves the era of old-style telephones and enters the Internet Age.

Emails are distinctly unlike land-line telephone calls in many respects, one being that an email may be sent or received anywhere that has an internet or cellular connection, using highly portable equipment – laptops with WiFi connections, tablets, and mobile phones. They travel from one @-sign “address,” wholly unrelated to any geographic location, to another.

As noted above, Google does not keep a record of a Gmail user’s residential address. More to the point, Google has no way of knowing where the account holder’s correspondent – the plaintiff in this case, for example – resides. Nor is there evidence that Google could know where either was situated when sending or receiving a particular email (see footnote 5), an issue on which, to whatever extent it may be relevant, the plaintiff has the burden of proof.

Applying the Massachusetts wiretap statute to Gmail communications sent to or from a Massachusetts resident or visitor – irrespective of where they might be scanned or processed – would thus make compliance a game of chance. Assuming that no responsible entity would risk a Massachusetts felony prosecution by scanning an email that *might* have been sent or received in Massachusetts or by a Massachusetts resident, the practical effect would be to regulate the practice nationwide. Some would undoubtedly view this as a desirable result; others would just as surely disagree. In either event, “a State may not impose economic sanctions on violators of its laws with the intent of changing the tortfeasors’ lawful conduct in other States.” BMW of North America, Inc. v. Gore, 517 U.S. 559, 573 (1996).

“A fundamental tenet of statutory interpretation is that statutory language should be given effect consistent with its plain meaning and in light of the aim of the Legislature unless to do so would achieve an illogical result.” Sullivan v. Brookline, 435 Mass. 353, 360 (2001). The Massachusetts wiretap statute says nothing, one way or the other, about extraterritorial application. Federal regulation is one thing,¹⁵ see Gore at 572, but there is no reason to suspect that the Massachusetts legislature intended, in 1968 or since, that our statute be applied to out-of-state conduct, especially where this would amount to a Massachusetts-imposed interdiction against a practice whose implementation occurs elsewhere and whose effects – good and bad – are worldwide.

¹⁵As it happens, a federal court in California is considering the legality of Google’s scanning and processing of emails under the federal ECPA, as well as California’s wiretap statute. In re: Google, Inc. Gmail Litigation, 2013 WL 5423918 (U.S. Dist. Ct., N.D. Cal., Sept. 26, 2013). So far, the plaintiffs have survived a motion to dismiss but lost their motion for class certification. The case is still pending.

The statute's criminal penalties are relevant for another reason as well. "The general rule, accepted as 'axiomatic' by the courts in this country, is that a State may not prosecute an individual for a crime committed outside its boundaries." Vasquez, petitioner, 428 Mass. 842, 848 (1999); see cases cited there and in Commonwealth v. Armstrong, 73 Mass. App. Ct. 245, 249 (2008).

To this general rule there is the narrow exception known as the "effects doctrine," under which "[a]cts done outside a jurisdiction, but intended to produce and producing detrimental effects within it, justify a State in punishing the cause of the harm as if he had been present at the effect." Strassheim v. Daily, 221 U.S. 280, 285 (1911; Holmes, J.).¹⁶ Assuming that users of non-Gmail accounts are detrimentally affected by Google's out-of-state scanning of emails, Google cannot be said to have "intended to produce" such effects within Massachusetts when it had no way of knowing where the sender or recipient of a particular email was located. As the Appeals Court observed in Armstrong, the effects doctrine is not "so broad as to empower a State to exercise jurisdiction where all acts in furtherance of the crime and all offense elements of the crime are committed wholly outside the borders of the State." 73 Mass. App. Ct. at 251.

For all of these reasons, I very much doubt that the Legislature, in 1986 or since, intended that the wiretap statute be applied to the out-of-state conduct at issue here. Google's Motion for Summary Judgment is therefore allowed.

¹⁶In Strassheim the respondent, a Chicago businessman, traveled to Michigan – the prosecuting jurisdiction – to deliver a bid, which a state authority signed in his presence, for the purchase of \$10,000 worth of new equipment; what was later delivered, however, was secondhand equipment. In Vasquez, the SJC applied the Strassheim rule to a Massachusetts father's failure to pay child support to his family in Oregon.

ORDER

For the foregoing reasons, the defendant's Motion to Dismiss is ALLOWED. Judgment to enter, dismissing the Complaint. The text of this decision other than the Order shall be impounded pending decision on any motion (joint if possible) for redaction, to be filed with a copy of the proposed redacted decision within 20 days of the date the Order is docketed.



Thomas P. Billings
Justice of the Superior Court

Dated: February 13, 2015

NOTICE IN HAND
06.19.14
A.K.+Z.

IMPOUNDED

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

**SUPERIOR COURT
SUCV2011-02808-BLS1**

DEBRA L. MARQUIS

vs.

GOOGLE, INC.

**MEMORANDUM OF DECISION AND ORDER ON
PLAINTIFF'S MOTION FOR CLASS CERTIFICATION**

On July 29, 2011, the plaintiff, Debra L. Marquis, individually and on behalf of those similarly situated, filed this action against the defendant, Google, Inc. She alleges that she is not a user of Google's email service—Gmail—and that Google violated the Massachusetts wiretap statute, G.L. c. 272, § 99 (wiretap statute), each time it reviewed the content of emails that she sent to Gmail users or Gmail users sent to her. Marquis claims that she, and all others similarly situated to her, are entitled to statutory damages at the rates set out in G.L. c. 272, § 99(Q), as well as declaratory and injunctive relief as a consequence of these violations of the wiretap statute. The case is presently before the court on Marquis' motion for class certification, pursuant to Mass. R. Civ. P. 23, in which she asks the court to certify a class of: "all Massachusetts residents who (1) did not have Gmail accounts at the time that they (2)(a) sent emails from their non-Gmail account email accounts to a Gmail account and/or (2)(b) received emails from a Gmail account (3) which emails Google scanned for their substantive content to use for its own commercial purposes (4) at any time from April 2004 (when Google first

introduced Gmail) to the present” Marquis contends that class certification is appropriate because Google processes “millions of emails within a limited number of identifiable categories in virtually identical manners.”

The parties have filed memoranda and also a number of affidavits with numerous exhibits attached in support of and in opposition to the motion for certification. In addition, Google has filed a related motion to strike the affidavit of Michael Helmstadter, a witness who the plaintiff submits is an expert able to describe the manner in which Google processes and reviews the content of emails and to render certain opinions in support of the plaintiff’s motion for class certification. That motion is addressed in a separate order.

On April 3, 2014, the court convened a hearing on the motions. In consideration of the parties’ pleadings, evidentiary submissions and oral argument, for reasons that follow, the plaintiff’s motion for class certification is DENIED.

BACKGROUND

The facts relevant to this motion, as revealed by the pleadings and other materials submitted by the parties, are as follows. See *Fletcher v. Cape Cod Gas Co.*, 394 Mass. 595, 597 (1985) (noting that court may consider relevant factual materials submitted by the parties on a motion to certify class action). See also *Weld v. Glaxo Wellcome Inc.*, 434 Mass. 81, 85-86 (2001).

In 2004, Google launched Gmail as a free web-based email service. Today, it has approximately 400 million users. As explained in more detail below, Gmail uses an automated processing system to scan the contents of emails to, among other things, detect spam and computer viruses, sort emails, and, of relevance to this case, deliver targeted advertising to Gmail users based on words in their emails. Google generates advertising revenue from Gmail by

selling advertisements targeted to the users by means of an automated review of email content. For example, if a Gmail user sends and receives emails about photography or cameras, he or she might see advertising from a local camera store.

Google Apps is a suite of integrated Google products that includes Gmail. Other Google Apps services include a calendar, online file storage, video and text messaging, and archiving services. Google Apps customers include businesses, educational organizations, and internet service providers that have contracted with Google for these services. The Google Apps customer's own system administrators, not Google, oversee the creation of email accounts and the drafting and implementation of terms of service, use policies, or privacy policies associated with users' email accounts; some Google Apps customers permit content review and targeted advertising, some do not. Generally, Google Apps email users do not have an email address that ends with "@gmail.com."

Marquis is a resident of Boxford, Massachusetts and works as a flight attendant for American Airlines. She has an email account with America Online (AOL) and has used her AOL email account to communicate with Gmail account users. Marquis claims that Google violated the wiretap statute by scanning the emails she exchanged with Gmail users without her consent. At a deposition on February 12, 2013, Marquis acknowledged that she has sent emails to Gmail users from her non-Gmail account even after she filed this action.

Declaration of Brad Chin & Google's Terms of Service and Disclosures

Google has submitted the declaration of Brad Chin, a senior privacy manager at Google since 2012. According to Chin, Google discloses information about its collection and processing of data in numerous ways, including through its terms of service, privacy policy, Gmail privacy notices, and Gmail legal notices. Google supplements these disclosures with information about

specific services on various web pages within Google's website, including "Help" pages and Google tools that allow users to customize their privacy and advertising settings. The language of these disclosures has evolved over the years, and in consequence, Gmail and Google Apps users who began using Gmail on different dates may have seen different disclosure language about Google's data practices when they opened their email accounts.

All Gmail users must agree to Google's terms of service and privacy policy before creating a Gmail account. Gmail legal notices and privacy notices have been incorporated into the terms of service and privacy policy. Gmail users create their accounts through Google's "Create an Account" page. This page has changed over time, but has consistently required users to click a box indicating that by opening a Gmail account, he or she will agree to be bound by Google's terms of service and privacy policy. At various times, this page has explained that, "[w]ith Gmail, you won't see blinking banner ads. Instead, we display ads you might find useful that are relevant to the content of your messages." By contrast, Google Apps users go through a different sign-up process through pages created by the Google Apps customer (e.g. a business or educational organization).

The April 16, 2007 version of Google's terms of service was in effect at the beginning of the putative class period and remained in effect through March 1, 2012. See Exhibit D to Chin Declaration. The April 2007 terms of service informed users that: "Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information." Services are defined as, "Google's products, software, services and web sites."

From October 14, 2005 to October 3, 2010, Google provided Gmail-specific privacy

disclosures that it incorporated into the Google privacy policy. The Gmail privacy notice dated October 14, 2005 explained that: "Google maintains and processes your Gmail account and its contents to provide the Gmail service to you and to improve our services. The Gmail service includes relevant advertising and related links based on the IP address, content of messages and other information related to your use of Gmail. Google's computers process the information in your messages for various purposes, including formatting and displaying the information to you, delivering advertisements and related links, preventing unsolicited bulk email (spam), backing up your messages, and other purposes relating to offering you Gmail."

In addition, Google maintains various publicly accessible "Help" pages. The language of these Help pages has changed over time. From June of 2009 to June of 2012, one Help page entitled, "Ads in Gmail and your personal data," stated:

Ads that appear next to Gmail messages are similar to the ads that appear next to Google search results and on content pages throughout the web. In Gmail, ads are related to the content of your messages. Our goal is to provide Gmail users with ads that are useful and relevant to their interest.

Ad targeting in Gmail is fully automated, and no humans read your email in order to target advertisements or related information. This type of automated scanning is how many email services, not just Gmail, provide features like spam filtering and spell checking. Ads are selected for relevance and served by Google computers using the same contextual advertising technology that powers Google's AdSense program.

Google's internal records indicate that this Help page received over [REDACTED] views from 2010 to 2012. From December of 2011 to December of 2012, another Help page explained:

Is Google reading my mail?

No, but automatic scanning and filtering technology is at the heart of Gmail. Gmail scans and processes all messages using fully automated systems in order to do useful and innovative stuff like filter spam, detect viruses and malware, show relevant ads, and develop and deliver new features across your Google experience. Priority Inbox, spell

checking, forwarding, auto-responding, automatic saving and sorting, and converting URLs to clickable links are just a few of the many features that use this kind of automatic processing.

Exhibit R to Chin Declaration. Additionally, Google's "Ad Preferences Manager" page was viewed approximately [REDACTED] times from 2010 to 2012. Declaration of Tobias Haamel dated Jan. 13, 2014.

Publicity Surrounding Launch of Gmail and its Scanning Processes

Ever since Google first introduced Gmail in 2004, there have been thousands of news articles, radio programs, blog posts, law review articles, and videos generated concerning Gmail's automated scanning features. See Declaration of Kyle Wong dated Jan. 17, 2014. According to Google, a search of news articles on Westlaw revealed that there are nearly 2,000 articles on the topic of Gmail's scanning of users' emails. A Google search of the term "Gmail scans email content" returned millions of results. The materials Google has submitted in opposition to the motion for class certification include a number of articles discussing this topic. These articles were published in Forbes, USA Today, U.S. News & World Report, the New York Times, Wired, the Washington Post, PCWorld, the Chicago Tribune, the Boston Globe, the Houston Chronicle, the Seattle Times, CNet.com, the Los Angeles Times, and the Wall Street Journal, among other newspapers and magazines, from 2004 to 2013. See Exhibits 2-73 of Wong Declaration. For example, the May 31, 2004 Boston Globe includes an article by Hiawatha Bray entitled "Google's Gmail is still a rough draft." It includes the following passage:

Much has been made of Google's plan to make money off the service by featuring ads inspired by the contents of the e-mail messages. Intrusive? Not really. Indeed, it's sort of cool. A note about the Bank of America merger with FleetBoston Financial Corp. spawns an ad from the Internet service Mapquest, offering to draw a map of all Fleet offices. An attack on firms that hire engineers from overseas features an ad seeking hosts for foreign

exchange students.

I took to checking the mail just to see what kind of advertisement would pop up. Again, that's just what Google wants. Unlike most ads, these relate to something that interests you, so you'll almost certainly read them.

At the same time, Gmail taps the Google Web index, posting links to sites with related information. These aren't ads, just a smattering of related Internet pages that can help you better understand the e-mail you're reading. This feature won't bring Google any revenue, but it's helpful enough to attract still more faithful users.

The ads and index links are in plain text, on the right side of the page. They're far less obtrusive than the gaudy flashing ads found on most free e-mail services. As for the threat to privacy, Google vows that it won't keep or sell any information it derives from scanning the e-mails. California's state senate just passed a bill that would make this policy mandatory. In all, the system offers much to admire and nothing to fear.

Gmail still needs lots of work, though. Start with its spam filtering. It's not very good. It seems to use a Bayesian approach the kind of filter that gets better at snuffing spam as more people use it. Google asks users to mark any spam that gets through, to help train the system. And the system needs plenty of help. Lots of spam messages are allowed to pass, while the occasional good message is filtered out.

...

So let's assume that Google improves Gmail's spam filtering and beefs up its features. Will it then be worth \$40 just to sign up? Of course not. By then, it'll probably be available for free. But in case you feel differently, I still have two unused Gmail invitations. Make an offer.

Exhibit 12 of Wong Declaration. An article from the New York Times by David Pogue dated May 13, 2004, entitled "STATE OF THE ART; Google Mail; Virtue Lies In the In-Box" has the following description of automated email review:

So six weeks ago, when Google described Gmail, the free e-mail service it is testing, the prevailing public reaction was shock. The company said that its software would place ads in your incoming messages, relevant to their contents.

It appeared to many people that Google had gone way beyond evil into Big Brother land. What could be more sinister than snooping through private correspondence looking for advertising opportunities?

Privacy advocates went ballistic. The Electronic Privacy Information Center called for

Gmail to be shut down, describing it as “an unprecedented invasion into the sanctity of private communications.” And a California state senator, Liz Figueroa, offered a bill that would make it illegal to scan the contents of incoming e-mail. (Never mind that such a bill would make it illegal for children’s e-mail services to filter out pornographic material.)

Those reactions, as it turns out, are a tad overblown. In fact, no human ever looks at the Gmail e-mail. Computers do the scanning -- dumbly, robotically and with no understanding the words -- just the way your current e-mail provider scans your messages for spam and viruses. The same kind of software also reads every word you type into Google or any other search page, tracks your shopping on Amazon, and so on.

Besides, if you’re that kind of private, Gmail is the least of your worries. You’d better make sure that the people at credit-card companies, mail-order outfits and phone companies aren’t sitting in back rooms giggling at your monthly statements. Heck, how do you know that your current e-mail providers -- or the administrators of the Internet computers that pass mail along -- aren’t taking an occasional peek?

Still, you feel what you feel. If Gmail creeps you out, just don’t sign up.

That would be a shame, though, because you’d be missing a wonderful thing. Even in its current, early state, available only to a few thousand testers, Gmail appears destined to become one of the most useful Internet services since Google itself.

Exhibit 7 of Wong Declaration.

Plaintiff’s Expert Michael Helmstadter’s Analysis of Google’s Email Practices

Marquis has submitted a thirteen-page affidavit from her expert, Michael Helmstadter. See Exhibit 2 to Affidavit of Jeffrey Thorn dated Feb. 14, 2014. The Helmstadter Affidavit explains that Helmstadter analyzed Google’s protocol for scanning emails sent between Gmail users and non-Gmail email users. Helmstadter has had over twenty years of experience in the analysis, development, and management of various computer systems, as well as experience in computer programming, database management, and companies’ software and hardware infrastructure administration. Helmstadter and fellow plaintiff’s expert, Jeffrey Page, have reviewed emails produced by Marquis, documents produced by Google, and deposition testimony. Helmstadter has also conducted his own independent testing and research concerning

Google's Gmail system and the underlying metadata. He avers that:

6. In order to better understand the processes Google uses to scan emails for commercial content, I, along with Jeffrey Page, have (1) conducted a variety of tests on Plaintiff's emails which were downloaded from her AOL email account to an Outlook program in order to review their metadata properties; (2) analyzed Gmail's incoming and outgoing emails and the javascript code present with the email, by using dedicated programs including Telerik Fiddler to reveal this data, while working within both existing and newly created "sterile" sample Gmail accounts; (3) analyzed the metadata attached to emails sent between non-Gmail users and Gmail users, in both Plaintiff's emails and various other accounts and emails created specifically to better understand Google's scanning process and the servers through which it runs; and (4) have tested the feasibility of using different types of software programs to search through email metadata for key terms and determine whether such searches could be conducted on a large-scale basis.

7. I have concluded that Google uniformly scans for commercial content those emails sent between Gmail email users and non-Gmail email users in certain circumstances. In this expert report, I provide an overview of relevant scanning issues and then address the following circumstances in which emails are uniformly scanned: (1) all emails which are assigned a smart label; (2) all emails sent to Gmail users [REDACTED] (i.e., all "incoming emails"); (3) all emails sent to Gmail users [REDACTED] which were opened by the Gmail user using Gmail's Web-Based Interface; (4) all emails sent from Gmail users [REDACTED] which were sent to non-Gmail users using a Web-Based interface.

8. These "sub-classes" of emails overlap—for example, (1) all emails assigned a smart label includes all (2) emails sent to Gmail users [REDACTED]—but the subclasses exclude any emails which have not been scanned by Google.

Helmstadter believes that Google has scanned billions of emails exchanged between Gmail users and non-Gmail users for their substantive content in order to extract commercial value and provide targeted advertising to the Gmail users. According to Helmstadter, the exact manner of Google's scanning for commercial purposes has evolved to become increasingly more "intrusive" since Gmail was originally made public. For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Google implemented the creation of a "User Modeling" system for individual Gmail users. This form of personalized advertising is based on an individual's User Model and is a collection of attributes and data based on the user's Gmail email contents as well as other factors. Helmstadter believes that all Gmail accounts are created with personalized advertising activated, Gmail's default setting. He believes that all Google Apps accounts [REDACTED]

[REDACTED]

Helmstadter opines that Google tracks whether companies have enabled advertising.

Google constructs the User Model of a Gmail user in a [REDACTED] [REDACTED] targeted advertising scanning. User Modeling takes place in a [REDACTED] [REDACTED] which scans the text body of an email for substantive information. By analyzing incoming and outgoing emails and the associated JavaScript, Helmstadter has concluded that

[REDACTED] See Exhibit E to Helmstadter Analysis.¹ [REDACTED]

[REDACTED] Google has used the User Model and targeted advertising to scan

¹ Exhibit E appears to show JavaScript from a message within Gmail (sent by Google to a Gmail user), not a non-Gmail account.

emails for substance and content [REDACTED]

[REDACTED] which advertisement would generate more revenue for Google and would select that advertisement to be displayed to a Gmail user.

In addition, Helmstadter believes that Google uniformly scans certain categories of emails for commercial purposes as follows: all emails which have been assigned a Google Smart label; all emails sent to Gmail users [REDACTED]; all emails sent to Gmail users prior to [REDACTED] which were opened by the Gmail user using Gmail's web-based interface; all emails sent from Gmail users [REDACTED] to non-Gmail users using a web-based interface; and emails sent to and from Google Apps clients. Helmstadter asserts that he can identify each category of emails through metadata or other records maintained by Google.

Helmstadter concludes that he has "done sufficient testing to confirm that a software program could be written and/or purchased and customized that would be able to search metadata (whether contained within the email or not) for key terms indicating whether a particular email residing in either the Class member's account or the relevant Gmail account was in violation of the Massachusetts Wiretapping Statute because Google had scanned the substantive content of such email for information that it could use to make a profit for itself."

Declaration of Stacey Kapadia and the Processing of Emails in Gmail

Google has submitted the twenty page declaration of Stacey Kapadia dated January 16, 2014 in opposition to the motion for class certification. Kapadia, a software engineer at Google, is familiar with Google's internal systems related to Gmail and general business decision-making and strategy related to these systems. Kapadia is aware that Marquis claims that Google "reads" all emails in four categories: (1) all emails that have Smart Labels associated with them; (2) all emails sent to a Gmail account [REDACTED]; (3) all emails sent to a Gmail account [REDACTED]

[REDACTED] that were opened by a Gmail account holder using Google's web-based interface/SMTP pathway; and (4) all emails sent from a Gmail account using Google's web-based interface/SMTP pathway to non-Gmail users after [REDACTED]. She refers to these categories of emails as Categories 1, 2, 3, and 4, respectively, throughout her declaration and disputes the claim that Google reads all these emails. Kapadia states that: "Google does not 'read' emails. Google employees do not review Gmail messages (except in rare circumstances with express user permission). Rather, Google applies automated processing to email messages to provide various services and features to users of the free Gmail service." Kapadia also asserts that in each of the categories identified by Marquis, Google's processing of email is not uniform, and the text of an email may or may not be scanned based on factors that differ from user to user and from message to message.

According to Kapadia, many emails are rejected and never delivered or scanned. [REDACTED]

[REDACTED] [REDACTED]

In order for Google's systems to receive an email from a non-Gmail user, the computer server transmitting the email must successfully exchange a series of command/reply sequences with Google's servers using the Simple Mail Transfer Protocol (SMTP). If those sequences are not successful,

[REDACTED]

[REDACTED]

Kapadia maintains that there are several additional exceptions to scanning that undermine Marquis' assertion that uniform scanning applied to the emails in Category 3, emails sent to a Gmail account [REDACTED] that were opened by a Gmail account holder using Google's web-based interface/SMTP pathway. The emails in Category 3 are associated with processing by Google's [REDACTED]

[REDACTED] According to Kapadia, [REDACTED] Gmail users. Google's [REDACTED] is used in certain circumstances to display relevant advertising [REDACTED]

[REDACTED] automated and does not involve human review. [REDACTED] processing applies, it operates by identifying words in an email that may be relevant for advertising purposes.

Google's systems subsequently attempt to match an advertisement to those words, which will be shown to the Gmail user when he or she views the email. [REDACTED]

[REDACTED] to Gmail users in numerous circumstances, and scanning was based on factors that varied for each email. For example, [REDACTED] occur in the following instances: [REDACTED]

[REDACTED]



According to Kapadia, [REDACTED]
which emails were [REDACTED]
apart from the emails themselves. Kapadia is [REDACTED]
[REDACTED]

[REDACTED] each individual email recipient. In an instance
where a non-Gmail user sends an email to a Gmail user, Kapadia [REDACTED]
[REDACTED]

[REDACTED]. Kapadia notes that [REDACTED]
[REDACTED] for most users as compared to the time period [REDACTED]

Moreover, the scanning of emails in Category 2, emails sent to Gmail users [REDACTED]

² [REDACTED] advertisements are shown in Gmail on mobile devices, [REDACTED]
[REDACTED]. The advertisements shown when emails are viewed on mobile devices [REDACTED]
[REDACTED]

[REDACTED] is also subject to various exceptions. The emails in Category 2 refer to emails subjected to [REDACTED], which was implemented [REDACTED]. [REDACTED] is an automated process that does not involve human review. For example, [REDACTED] the dates of events referenced in the text of emails and enables Gmail users to click the date and automatically create a reminder in the user's calendar. [REDACTED] shipping notifications with package tracking information and enables Gmail users to click a button that takes them to the shipping company's website to track their shipments. [REDACTED] in some circumstances to assign a "Smart Label" to an email in a sectioned Gmail inbox. In a sectioned inbox, emails are automatically sorted into various categories, such as, "Primary," "Social," "Promotional," "Updates," and "Forums." These categories are automatically assigned based on various characteristics of the email, some of which are derived [REDACTED].

Gmail users have the option of opting out of personalized advertising on Google's website and information identified [REDACTED] for those particular users. If the user has not opted out of personalized advertising and if a user accesses Gmail in a manner that displays advertising, then the information obtained from a number of the user's most recent emails and additional basic data concerning the user are harvested in a [REDACTED]. This collective information is used to select and display ads to the Gmail user.

[REDACTED] is not applied to all emails sent to Gmail users. [REDACTED], an email received by a Gmail email account generally [REDACTED]. Although many [REDACTED].

approximately [REDACTED]

[REDACTED] that would, in turn, impact whether a particular email is actually scanned. [REDACTED]

Google [REDACTED] themselves. A non-Gmail user could not review his or her own email account to determine whether an email was [REDACTED] because Google's systems do not provide any information to the non-Gmail sender that reflects scanning.

As to Category 1 emails, emails assigned a Smart Label, Kapadia asserts that these emails have not necessarily been scanned for commercial content. She disputes Helmstadter's conclusion that [REDACTED]

[REDACTED] According to Kapadia, even if JavaScript coding is present with respect to a particular email, it would [REDACTED] that the contents of an email were scanned for purposes of displaying advertisements. For instance, [REDACTED] even though no scanning of email content has occurred.

Kapadia also disputes Helmstadter's conclusion that all emails in Category 4, emails sent from a Gmail account using Google's web-based interface/SMTP pathway to non-Gmail users [REDACTED], are uniformly scanned. She notes that the [REDACTED]; rather, [REDACTED] come from emails. Google does [REDACTED] about which emails were processed by [REDACTED]

the [REDACTED]
[REDACTED].

Kapadia notes that Google Apps email users present further individualized issues relating to whether emails are scanned. Some Google Apps users may have advertising disabled entirely for their accounts, depending on settings chosen by their account managers. If advertising is disabled, then [REDACTED] the Google Apps accountholder. Also, if advertising is disabled, [REDACTED] for a user, [REDACTED] the user has chosen to opt out of personalized advertising.

Finally, Kapadia notes that Google [REDACTED]
[REDACTED]
[REDACTED]. For instance, Google [REDACTED]
[REDACTED]
[REDACTED]. Gmail users are not required to identify their state of residency in order to create a Gmail account.

Declaration of Brandon Long and Google Apps

Google has also submitted the declaration of Brandon Long, a software engineer at Google familiar with Google Apps. Google Apps allows customers to customize their Google Apps email account by directing emails sent to their end users to be processed over their own systems, rather than Google's systems. This can be implemented in a number of different ways, but some result in no COB processing. Customers can configure these settings, and these settings may vary with respect to a particular Google Apps customer. For example, a Google Apps customer may initially use Google's systems to process emails sent to its end users and then eventually transfer processing to its own systems.

Long is not aware of any data source or method that could be used to identify the Google Apps customers that configured their Google Apps accounts to avoid COB processing without reviewing information specific to each individual Google Apps customer. Moreover, according to Long, Google does not keep records about which Google Apps customers use their own systems to process email messages in place of Google's systems.

After reviewing portions of Google's code, Long disputes Helmstadter's assertion that "all Google Apps accounts until approximately 2011 were created with advertising activated at the corporate domain level and, at the individual user settings level with User Modeling and personalized advertising enabled." He points out that Google Apps for Business has always had advertising disabled by default and whether advertising was ever activated depends on the choices a Google Apps customer makes when setting up and maintaining the account.

DISCUSSION

This court has broad discretion in determining whether to certify a class action. *Salvas v. Wal-Mart Stores, Inc.*, 452 Mass. 337, 361 (2008). The court, however, may not grant class status on the basis of speculation or generalization regarding the satisfaction of the requirements of Mass. R. Civ. P. 23, or deny class status by imposing, at the certification stage, the burden of proof that will be required of the plaintiffs at trial. *Weld v. Glaxo Wellcome Inc.*, 434 Mass. 81, 84-85 (2001). "The standard defies mathematical precision" *Id.* at 85.

Under Mass. R. Civ. P. 23, the plaintiff must show that (1) the class is sufficiently numerous to make joinder of all parties impracticable, (2) there are common questions of law and fact, (3) the claims or defenses of the representative party are typical of the claims or defenses of the class, and (4) the named plaintiff will fairly and adequately protect the interests of the class. See Mass. R. Civ. P. 23(a). Moreover, the plaintiff must show that common

questions of law and fact predominate over individualized questions and that the class action is superior to other available methods for fair and efficient adjudication of the controversy. See Mass. R. Civ. P. 23(b). Under Mass. R. Civ. P. 23, a party moving for class certification is only required to provide “information sufficient to enable the motion judge to form a reasonable judgment” that certification requirements are met. *Aspinall v. Philip Morris Cos.*, 442 Mass. 381, 392 (2004) (citation omitted).

Federal case law suggests that there is another element that must be established before a class may be certified, that is that the class is “ascertainable.” In *Donovan v. Philip Morris USA, Inc.*, 268 F.R.D. 1, 9 (D. Mass. 2010), a Federal District Court described this requirement as follows: “While not explicitly mentioned in Rule 23, an implicit prerequisite to class certification is that a ‘class’ exists—in other words, it must be administratively feasible for the court to determine whether a particular individual is a member To be ascertainable, all class members need not be identified at the outset; the class need only be determinable by stable and objective factors.” *Donovan v. Philip Morris USA, Inc.*, 268 F.R.D. at 9 (internal quotations and citations omitted). However, when “class members [are] impossible to identify prior to individualized fact-finding and litigation, the class fails to satisfy one of the basic requirements for a class action under Rule 23.” *Shanley v. Cadle*, 277 F.R.D. 63, 68 (D. Mass 2011). See also *Kwaak v. Pfizer, Inc.*, 71 Mass. App. Ct. 293, 300-301 (2008) (where class certification was reversed when individual proof would be required to determine whether a particular purchaser of Listerine was exposed to deceptive advertising that affected the decision to purchase the product as the advertising was not uniform during the class period).

Marquis, of course, asserts that all of the Rule 23 prerequisites for class certification are met and her proposed class is ascertainable. Google opposes class certification on the grounds

that the plaintiff's proposed class is unascertainable and overbroad and because individual issues overwhelmingly predominate.³ In particular, Google contends that because of the wide publication of the fact that Google uses automated processes to scan emails for content to deliver targeted advertising as a means of generating revenue from the email service that is free to Gmail users, publication both by Google itself as well as in articles written by independent journalists, there is a paramount individualized question of fact that must be adjudicated with respect to every potential class member: Did the non-Gmail email user know that Google would perform this automated content review when he or she sent or received an email from a Gmail user such that the non-Gmail user could be said to have consented to this content review? For the reasons that follow, the court agrees with Google that this individual question of fact predominates for most, if not all, putative class members. The court therefore need not address the question of whether a class is ascertainable, although it will briefly discuss this issue.

Predominance

Under Mass. R. Civ. P. 23(b), the plaintiff must show that common questions of law and fact predominate over individualized questions, and that the class action is superior to other available methods for fair and efficient adjudication of the controversy. See Mass. R. Civ. P. 23(b). See also *Salvas v. Wal-Mart Stores, Inc.*, 452 Mass. at 363 ("The predominance test expressly directs the court to make a comparison between the common and individual questions involved in order to reach a determination of such predominance of common questions in a class

³ Google also asserts that Marquis is not an adequate class representative. As noted during oral argument, in a case of this sort, the fact that the named plaintiff does not understand the legal theories for the claim asserted by her attorney will seldom preclude class certification where the attorneys are competent to represent the class and the plaintiff understands her representative role. In any event, because the court has denied class certification for other reasons, this issue need not be further addressed.

action context”) (citation omitted). The predominance requirement is satisfied by a sufficient constellation of common issues between class members and cannot be reduced to a mechanical, single-issue test. See *Weld v. Glaxo Wellcome Inc.*, 434 Mass. at 92. See also *Waste Mgt. Holdings, Inc. v. Mowbray*, 208 F.3d 288, 296 (1st Cir. 2000).

After the parties filed their pleadings and evidentiary materials in support of and in opposition to the motion for class certification, but prior to the April 3, 2014 hearing on the motion, Judge Lucy H. Koh of the United States District Court for the Northern District of California issued a decision denying, with prejudice, a motion for class certification in a consolidated multi-district litigation in which various plaintiffs brought similar claims against Google as those now before this court. See *In re Google Inc. Gmail Litigation*, No. 13-MD-02430, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014). In those consolidated putative class actions, the plaintiffs claimed that Google violated state and federal antiwiretapping laws in its operation of Gmail by intercepting and reviewing emails over a period of several years. They asserted causes of actions under “(1) the Electronic Communications Privacy Act of 1985 (“ECPA” or “the Wiretap Act”), 18 U.S.C. §§ 2510 *et seq.* (2012); (2) California’s Invasion of Privacy Act (“CIPA”), Cal. Penal Code §§ 630 *et seq.* (West 2014); (3) Maryland’s Wiretap Act, Md. Code Ann., Cts. & Jud. Proc. § 10-402 (West 2013); and (4) Florida’s Wiretap Act, Fla. Stat. Ann. § 934.01 (2013).” *Id.* at *1. The plaintiffs moved to certify four classes and three subclasses. In opposition, Google argued that none of the proposed classes satisfied the ascertainability, predominance, and superiority requirements. The court denied class certification because the plaintiffs failed to satisfy the predominance requirement. It held “that individual issues regarding consent are likely to overwhelmingly predominate over common issues” as “there is a panoply of sources from which email users could have learned of Google’s

interceptions other than Google's TOS and Privacy Policies." *Id.* at *17. For example, individuals could have learned about Google's interceptions of email from the news media, from Google itself, and from other sources, and the court noted that these sources were relevant to the question of whether consent to the alleged interceptions should be implied from the surrounding circumstances. *Id.* at *19. The court explained the reasons for its holding as follows:

Some Class members likely viewed some of these Google and non-Google disclosures, but others likely did not. A fact-finder, in determining whether Class members impliedly consented, would have to evaluate to which of the various sources each individual user had been exposed and whether each individual "knew about and consented to the interception" based on the sources to which she was exposed. See *Berry*, 146 F.3d at 1011. This fact-intensive inquiry will require individual inquiries into the knowledge of individual users. Such inquiries—determining to what disclosures each Class member was privy and determining whether that specific combination of disclosures was sufficient to imply consent—will lead to numerous individualized inquiries that will overwhelm any common questions.

Id. at *18. While the court's decision in *In re Google Inc. Gmail Litigation* does not expressly address the Massachusetts wiretap statute, and, in any event not binding on this court, for the reasons discussed below, this court finds Judge Koh's reasoning persuasive.

Before turning to the issue of predominance under the Massachusetts wiretap statute, it is useful briefly to identify certain questions that this case presents, but that the court need not decide at the class certification stage of the litigation. First, no Massachusetts appellate court has yet specifically held that emails are covered by the Massachusetts wiretap statute (see *Commonwealth v. Moody*, 466 Mass. 196, 207-209 (2013) (where text messages are held to be covered by the statute because they are communications transmitted with the aid of wire, cable or other like connection)), and even if they are, Google's automated review of emails for words that may link to targeted advertising may be exempt. For example, an essential component of any act in violation of the statute is the use of an intercepting device, and G.L. c. 272, § 99(B)(3) defines

“intercepting device.” That definition is initially quite broad, “any device or apparatus which is capable of transmitting, receiving, amplifying or recording a wire or oral communication,” but within that category of devices, the statute excludes “any telephone or telegraph instrument, equipment, facility, or a component thereof . . . , being used by a communications common carrier in the ordinary course of business.” Query whether Google’s servers that routinely scan email for spam, viruses, and content for keywords but not substance fit this exception?

Turning then to the question of whether for the plaintiff’s proposed class common questions of fact predominate over individualized questions, the court begins by considering the facts that a putative class member must prove to establish a violation of the Massachusetts wiretap statute. Our wiretap statute is framed largely in negative terms: surreptitious “interception” of any “wire or oral communication” “by any person (private citizen or public official) is proscribed, except as specifically provided in a few narrow exceptions . . . As defined by the statute, the term ‘interception’ ‘means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication.’” See *Commonwealth v. Tavares*, 459 Mass. 289, 296 (2011). The core of the statute is thus, the prevention of the *secret* interception of wire communications, i.e., an interception that is *secret* as to at least one of the participants. Indeed, in an early case construing the wiretap statute, *Commonwealth v. Jackson*, 370 Mass. 502, 505 (1976), the Supreme Judicial Court (SJC) explained that “it is clear that the Legislature intended that the statutory restrictions be applicable only to the *secret* use of such devices. (See § 99 A, and see § 99 B 4 which defines the term ‘interception’ to include ‘to secretly hear [or to] secretly record.’)” (emphasis supplied). In consequence, if a recording is “not made secretly,” it does

“not constitute an ‘interception’” and there has been no violation of the statute.

The facts of *Jackson*, while quite different from the facts of this case, are nonetheless instructive. In *Jackson*, the defendant had kidnapped his victim. He placed a series of telephone calls to the victim’s brother to convince him that he held the victim. The brother jury-rigged a recording device to the telephone and recorded the defendant’s calls. During two of the several calls, the defendant expressly stated that he knew the call was being taped or the line tapped, but nonetheless went on to discuss the kidnapping. After his indictment, the defendant moved to suppress the telephone call recordings, but the trial court denied the motion as it related to the two calls in which the defendant said that he knew the call was being recorded or the telephone “tapped.” The defendant argued that even though he had stated that he knew that he was being recorded, this was only surmise on his part, as he had not been expressly informed that he was being taped or tapped during the telephone conversation. The SJC rejected that argument. It agreed with the defendant that he had to have “actual knowledge” that he was being taped, but that knowledge could be proved with evidence other than an express statement made during the call by the brother that the call was being taped.⁴ A person’s “words and conduct” are “objective factors” from which actual knowledge of an “interception” can be determined and therefore whether it was actually secret. *Id.* at 507. Similarly, in this case, a plaintiff class member will have to prove that Google’s automated review of the contents of an email were unknown, i.e., “secret” as to him or her.

⁴ The plaintiff suggests that *Jackson* can be read to hold that the conversations in which the defendant did not expressly state that he knew the telephone was “tapped” could not be recorded without violating the statute. The trial court only suppressed the two statements in which the defendant commented on the taping and the defendant was convicted. The SJC made clear in its opinion that the appeal addressed only the two calls that the trial judge did not suppress. *Id.* at 505.

The plaintiff argues that a decision of the First Circuit Court of Appeals, *Campiti v. Walonis*, 611 F.2d 387 (1st Cir. 1979), stands for the proposition that consent must be express and can never be implied by objective factual evidence. Such a statement would be inconsistent with *Jackson*, but in any event, it is not what the *Campiti* court held. The question of whether “implied consent” is adequate to establish that the interception of a telephone call is not secret depends on what one means by the term “implied consent.” In *Campiti*, the First Circuit held that it is not enough to show simply that a person “should have known his call would probably be monitored and he, therefore, gave consent.” *Id.* at 393. Under those circumstances, where proof of actual knowledge was not forthcoming, consent cannot be implied. However, where objective evidence establishes, as a question of fact, that a person knew that a call was being “intercepted,” the interception was not secret and did not violate the statute.

In *In re Google Inc. Gmail Litigation*, Judge Koh used the term “implied consent” as a means of distinguishing the situation in which a person knew that the emails were being reviewed by Gmail and therefore impliedly consented to the practice when she exchanged emails with a Gmail user, from “express consent” which occurred when a Gmail user accepted terms of service that expressly stated that an automated content review would occur. Whether the non-Gmail user, who had not clicked agreement with terms of service describing the review, nonetheless knew about the automated content review was a question of fact. As Judge Koh explained, “courts have consistently held that implied consent is a question of fact that requires looking at all of the circumstances surrounding the interceptions to determine whether an individual knew that her communications were being intercepted.” *In re Google Inc. Gmail Litigation*, 2014 WL 1102660 at *16. Indeed, among the cases that Judge Koh cited in support of that comment was a First Circuit decision, *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-117 (1st

Cir. 1990), in which the court explained that “implied consent is not constructive consent. Rather, implied consent is ‘consent in fact’ which is inferred from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance. . . . [t]he circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private.” *Griggs-Ryan v. Smith*, 904 F.2d at 116-117 (internal citations and quotations omitted). While *Griggs-Ryan* addressed the federal wiretap statute, these comments on the fact-based inquiry concerning knowledge are equally applicable to this case.

As noted above, Google was never secretive about its automated review of emails. In this case, the factual record before the court documents the numerous opportunities that any potential class member had to become exposed to disclosures concerning the fact that Google conducted an automated review of emails to deliver targeted advertising to Gmail users. In consequence, with respect to any non-Gmail email user who exchanged emails with a Gmail user, the first factual question that must be confronted is: Did that person know about Google’s automated email review? For some putative class members, the resolution might be entirely documentary; if for example, they had or still have a Gmail account, in addition to the non-Gmail email service, and accepted terms of service that expressly explained the Google review. For many class members, however, the resolution of this question may turn on individualized evidence such as the extent of their use of the internet and technical sophistication and involve issues of credibility.

This same type of individualized factual inquiry necessary in this case precluded class certification in *Kwaak v. Pfizer, Inc.*, as discussed *infra*. There, the defendant employed

advertising for a period of time that suggested that Listerine was a substitute for flossing. This was alleged to be deceptive. During the class period, however, not all of the defendant's advertising included this assertion. In reversing the trial court's order certifying a class, the Appeals Court stated:

The class proposed to be certified therefore includes some consumers with exposure and some without exposure to a variety of different advertisements, some deceptive, for at least a category of consumers, and others adequately informative for any reasonable consumer. The class would include those who purchased the product for reasons related to the deceptive aspects of the advertising and those who purchased it for reasons totally unrelated. In these circumstances, it is difficult to conclude that the class certified consists of consumers similarly situated and similarly injured by a common deceptive act or practice.

Kwaak v. Pfizer, Inc., 71 Mass. App. Ct. at 301. Similarly, in this case, the proposed class undoubtedly includes many non-Gmail users who fully understood that Google monetized its Gmail service, which was free to all users, by delivering targeted advertising based on scanning email content. Determining which potential class members were aware of this practice would involve the same type of factual inquiry as would be required to determine which customers purchased Listerine in reliance on a deceptive ad and which did not.

In this case, as in *Kwaak*, the plaintiff looks for support in the SJC's decision, *Aspinall v. Philip Morris Companies, Inc.*, 442 Mass. 381 (2004), in which the SJC directed that a class of purchasers of Marlboro Light cigarettes be certified. In her reply brief, the plaintiff makes the following assertion: "[The SJC upheld] class certification even though 'plaintiffs have no chance of demonstrating that every class member was injured,'" citing pages 393-394 of the opinion. The quoted language, however, refers not to the SJC's reasoning, but to the defendant's contention, a factual contention that the SJC expressly rejected. On that point, the SJC made clear that the class was certified with respect only to economic damages which, if proved, would

be exactly the same for each class member so that no individualized inquiry of class members would be required. *Id.* at 397-400. As the SJC explained, the common question of fact that was predominant and made a class action the superior means for litigating the dispute was whether the defendant's conduct was deceptive. That question was "to be answered on an objective basis and not by the subjective measure [individualized to each smoker] argued by the defendants." *Id.* at 394. Here, there is nothing inherently deceptive in Google's protocol which it repeatedly disclosed and explained in public fora. The question of whether a particular class member had been exposed to these disclosures is clearly individualized. In this case, class members cannot be identified without an individualized inquiry.

Google Apps and Ascertainability

The plaintiff suggests in a letter to the court dated April 9, 2014 that a subclass could be certified that included only non-Gmail email users who exchanged email with individuals who had email services provided through a Google Apps customer. The plaintiff rightfully points out that the Google Apps email addresses do not have an "@gmail.com" suffix, therefore, a non-Gmail user would not be aware that the email user with whom he/she was corresponding was, in effect, a Gmail user and therefore his/her emails were being reviewed for purposes of targeted advertising. Therefore, as to such a Google Apps user, there could be no implied consent, absent proof that the non-Gmail correspondent was nonetheless aware that the Google Apps customer had enabled targeted advertising on email accounts. The short answer to the plaintiff's request is that it is inappropriate to raise this new subclass issue in a letter delivered to the court after the parties have filed their memoranda and evidentiary materials. This is particularly inappropriate when the question is no longer certification of subclasses, but rather whether this proposed subclass will be the only class certified.


The court, however, does not foreclose the plaintiff from pursuing such a class, although certain substantial impediments to certification do suggest themselves. First, the record presently before the court appears to establish that many Google Apps customers do not permit Google to place advertising on their email accounts, so those customers would not be conduits for unlawful, secret interception of emails. Moreover, if it were feasible to identify the Google Apps customers who permitted advertising, Marquis would had to have emailed someone who used such an email account. Marquis could not be a class representative of a class of which she is not a member. See *Doe v. The Governor*, 381 Mass. 702, 704-705 (1980) (noting that “if the individual plaintiffs may not maintain the action on their own behalf, they may not seek relief on behalf of a class”).

The court also has concerns regarding whether it would be possible to ascertain who the members of such a class are, *i.e.*, a class of Massachusetts email users who send and/or receive emails from an email account established through a Google Apps customer, who permits targeted advertising, and where that email user’s email address does not identify the applicable email server as a Google server. It seems unlikely that Google would have data which could be mined to identify potential class members. In *Carrera v. Bayer Corp.*, 727 F.3d 300, 306-307 (3rd Cir. 2013), the Third Circuit Court of Appeals explains the concept of ascertainability at length and its importance in determining whether a class may be certified. As noted earlier, Massachusetts’ own appellate courts have yet to weigh in on this implicit requirement for class certification, but the Third Circuit’s analysis has much to recommend it. If a plaintiff, such as Marquis, brought an individual claim, she would have to prove that her email was secretly intercepted. “A defendant in a class action has a due process right to raise individual challenges and defenses to claims, and a class action cannot be certified in a way that eviscerates this right or masks

individual issues . . . A defendant has a similar, if not the same, due process right to challenge the proof used to demonstrate class membership as it does to challenge the elements of a plaintiff's claim." *Id.* at 307. In sum, the *Carrera* decision suggests caution when a putative class "cannot be ascertained from a defendant's own records" unless a "reliable, administratively feasible alternative" is demonstrated. *Id.* at 304. The court was skeptical of approving an approach to identifying class members that amounted "to no more than ascertaining by potential class members' say so." *Id.* For that reason, it found class member affidavits an unacceptable method for establishing class membership. *Id.* at 309. Moreover, unlike some cases in which the "low value" of potential individual recoveries would discourage class members from going to the trouble to submit false claims, in a civil action for violation of the Massachusetts wiretap statute, the *minimum* recovery for each claimant is \$1000 (G.L. c. 272, § 99(Q)). See *Carrera v. Bayer Corp.*, 727 F.3d at 308-309 (where the court considers and rejects affidavits as a means of identifying class members even though individual recoveries would be modest). Cf. *Donovan v. Philip Morris USA, Inc.*, 268 F.R.D. 1 (D. Mass. 2010) (where the defendant had much data on longtime customers, only two easily identifiable personal characteristics were necessary for class member status—long term smoking and no diagnosis of cancer, and there was no monetary relief available for class members).

ORDER

For the foregoing reasons, the plaintiff's motion for class certification is **DENIED** with prejudice, except with respect to a possible class of non-Gmail email users that exchanged emails with an email user whose email service was provided by a Google Apps customer who permitted targeted advertising; and as to such a possible class, the court makes no ruling.



Mitchell H. Kaplan
Justice of the Superior Court

Dated: June 19, 2014

CERTIFICATE OF COMPLIANCE

I, Jeffrey Thorn, hereby certify that the foregoing Brief complies with the rules of the court that pertain to the filing of briefs, including, but not limited to:

Mass. R. A. P. 16(a)(6) (pertinent findings or memorandum of decision);

Mass. R. A. P. 16(e) (references to the record);

Mass. R. A. P. 16(f) (reproduction of statutes, rules, and regulations);

Mass. R. A. P. 16(h) (length of briefs and reply briefs); and

Mass. R. A. P. 20 (form of briefs, appendices, and other papers).

Respectfully submitted,

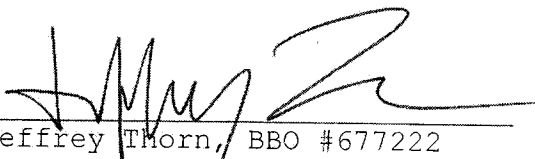


Jeffrey Thorn BBO #677222
ADKINS, KELSTON & ZAVEZ, P.C.
90 Canal Street, Suite 500
Boston, MA 02114
(617) 367-1040
jthorn@akzlaw.com

Dated: October 2, 2015

CERTIFICATE OF SERVICE

I, Jeffrey Thorn, hereby certify under the pains and penalties of perjury that two copies of Plaintiff's Opening Brief and the Parties' Joint Appendix were served on counsel of record for the appellee, including Robert B. Lovett, Esq., via **electronic mail and hand delivery** at Cooley LLP, 500 Boylston St., Boston, MA 02116 on this 2nd day of October, 2015.



Jeffrey Thorn, BBO #677222
ADKINS, KELSTON & ZAVEZ, P.C.
90 Canal Street, Suite 500
Boston, MA 02114
(617) 367-1040
jthorn@akzlaw.com

Dated: October 2, 2015