

Redacted Version

COMMONWEALTH OF MASSACHUSETTS

Appeals Court

No. 2015-P-0901

Suffolk Superior Court Civil Action No. 2011-2808-BLS1

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

DEFENDANT-APPELLEE/CROSS-APPELLANT'S OPENING BRIEF

(CONTAINS REFERENCE TO IMPOUNDED MATERIALS)

Michael G. Rhodes (*pro hac vice*)
Whitty Somvichian (*pro hac vice*)
Kyle C. Wong (*pro hac vice*)
Karen L. Burhans (BEO 679017)
COOLEY LLP
101 California Street, 5th Flr.
San Francisco, CA 94111-5800
Tel: (415) 493-2000
Fax: (415) 493-2222
rhodesmg@cooley.com
wsmovichian@cooley.com
kwong@cooley.com
kburhans@cooley.com

Counsel continued on signature
page

Dated: December 18, 2015

Debra L. Marquis v. Google Inc., No. SJC-12103

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21(b)(i), Google Inc. states that it is a wholly owned subsidiary of Alphabet Inc., a publicly held corporation: Accordingly, Alphabet Inc. has more than 10% ownership of Google Inc.

TABLE OF CONTENTS

	Page
CORPORATE DISCLOSURE STATEMENT.....	i
STATEMENT OF THE ISSUES.....	1
STATEMENT OF THE CASE.....	1
I. PRIOR PROCEEDINGS.....	1
II. STATEMENT OF THE FACTS.....	1
A. Google's Gmail Service.....	1
B. Google's Disclosures Of Its Automated Processing.....	4
C. Google Has No Way Of Identifying Members Of Plaintiff's Proposed Class.....	5
SUMMARY OF ARGUMENT.....	5
ARGUMENT.....	8
III. THE TRIAL COURT PROPERLY GRANTED SUMMARY JUDGMENT DISMISSING PLAINTIFF'S CLAIM.....	8
A. The Act Does Not Apply To Google's Conduct Outside Of Massachusetts.....	8
1. The Wiretap Act Is A Criminal Statute Subject To The Presumption Against Extraterritorial Application.....	8
2. Choice-Of-Law Principles Confirm That The Wiretap Act Does Not Apply Here.....	13
3. Extraterritorial Application Of The Act Would Violate The Dormant Commerce Clause.....	16
B. Alternative Bases For Affirming The Trial Court's Summary Judgment Decision.....	20
1. The OCB Exception.....	20

TABLE OF CONTENTS
(continued)

	Page
a. The OCB Exception Applies Because Google's Automated Scanning Has A Legitimate Business Purpose.....	20
b. The OCB Exception Is Not Limited To The Employer-Employee Context.....	25
c. The Communications Common Carrier Element Does Not Bar Google From Invoking The OCB Exception.....	27
d. Plaintiff Fails To Show That Google's Automated Scanning Is Not A "Legitimate Business Purpose.".....	29
2. The Court Did Not Err In Denying Partial Summary Judgment For Plaintiff.....	33
IV. THE TRIAL COURT PROPERLY DENIED PLAINTIFF'S MOTION FOR CLASS CERTIFICATION.....	36
A. Individuals Who Impliedly Consent To Google's Automated Scanning Have No Claim.....	36
B. The Trial Court Properly Held That The Issue Of Implied Consent Is Individualized.....	38
C. Plaintiff's Response To The Individualized Issues Of Knowledge Is Meritless.....	41
D. Alternative Bases For Affirming The Trial Court's Denial Of Class Certification.....	44

TABLE OF CONTENTS
(continued)

	Page
1. Plaintiff Cannot Identify The Instances Of Scanning On A Classwide Basis.....	44
2. The Proposed Class Is Unascertainable.....	45
E. The Court Properly Refused To Certify A Sub-Class Of Google Apps Users.....	47
V. THE TRIAL COURT ERRED IN DENYING GOOGLE'S MOTION TO DISMISS.....	49
A. Google's Conduct Is Excepted From Liability Under The OCB Exception To The Act.....	49
CONCLUSION.....	50

TABLE OF AUTHORITIES

	Page (s)
Cases	
<i>Adams v. City of Bos.</i> , 461 Mass. 602 (2012)	29
<i>Am. Booksellers Found. v. Dean</i> , 342 F.3d 96 (2d Cir. 2003)	18
<i>Am. Civil Liberties Union v. Johnson</i> , 194 F.3d 1149 (10th Cir. 1999)	19
<i>Baird v. Attorney Gen.</i> , 371 Mass. 741 (1977)	12
<i>BMW of N. Am., Inc. v. Gore</i> , 517 U.S. 559 (1996)	17, 18
<i>Boone v. Commerce Ins. Co.</i> , 451 Mass. 192 (2008)	33
<i>Bushkin Assocs., Inc. v. Raytheon Co.</i> , 393 Mass. 622 (1985)	13, 16
<i>Campiti v. Walonis</i> , 611 F.2d 387 (1st Cir. 1979)	37
<i>Carrera v. Bayer Corp.</i> , 727 F.3d 300 (3rd Cir. 2013)	47
<i>Chin v. Merriot</i> , 470 Mass. 527 (2015)	8
<i>Comm’r of Correction v. Super. Ct. Dept. Cty. of Worcester</i> , 446 Mass. 123 (2006)	25
<i>Com. v. Armstrong</i> , 73 Mass. App. Ct. 245 (2008)	9
<i>Com. v. Fafone</i> , 416 Mass. 329 (1993)	9

TABLE OF AUTHORITIES
CONTINUED

	Page(s)
<i>Com. v. Graham</i> , 388 Mass. 115 (1983)	8
<i>Com. v. Jackson</i> , 370 Mass. 502 (1976)	passim
<i>Com. v. Maccini</i> , No. 06-cr-0873, 2007 WL 1203560 (Mass. Super. Ct. Apr. 23, 2007)	10, 37
<i>Com. v. Marchionda</i> , 385 Mass. 238 (1982)	48
<i>Com. v. Rivera</i> , 445 Mass. 119 (2005)	43
<i>Com. v. Tibbs</i> , No. 01-cr-10170, 2007 WL 4644818 (Mass. Super. Ct. Jan. 4, 2008)	9
<i>Com. v. Vega</i> , 449 Mass. 227 (2007)	10
<i>Com. v. Wilcox</i> , 63 Mass. App. Ct. 131 (2005)	9
<i>Crandon v. U.S.</i> , 494 U.S. 152 (1990)	11
<i>Crosland v. Horgan</i> , 401 Mass. 271 (1987)	22, 26
<i>Dillon v. Mass. Bay Transp. Auth.</i> , No. 96-cv-4871, 1998 WL 128998, at *2 (Mass. Super. Ct. Mar. 19, 1998)	34
<i>Dillon v. Mass. Bay Transp. Auth.</i> , 49 Mass. App. Ct. 309 (2000)	21, 27, 28, 33
<i>Flesner v. Tech. Commc'ns Corp.</i> , 410 Mass. 805 (1991)	36

TABLE OF AUTHORITIES
CONTINUED

	Page(s)
<i>G.S. Enters., Inc. v. Falmouth Marine, Inc.</i> , 410 Mass. 262 (1991)	35
<i>Gilday v. Dubois</i> , 124 F.3d 277 (1st Cir. 1997)	22, 26
<i>Glik v. Cunniffe</i> , 655 F.3d 78 (1st Cir. 2011)	43
<i>In re Google Inc. Gmail Litig.</i> , No. 13-md-2430, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013)	23
<i>In re Google Inc. Gmail Litig.</i> , 13-md-2430, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014)	39
<i>In re Google, Inc. Privacy Policy Litig.</i> , No. 12-cv-1382, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012)	22, 23, 24, 29
<i>Griggs-Ryan v. Smith</i> , 904 F.2d 112 (1st Cir. 1990)	37
<i>Hall v. EarthLink Network, Inc.</i> , 396 F.3d 500 (2d Cir. 2005)	23, 24, 26, 29, 33
<i>Healy v. Beer Inst.</i> , 491 U.S. 324 (1989)	16
<i>Heffernan v. Hashampour</i> , No. 09-cv-2060, 2009 WL 6361870 (Mass. Super. Ct. Dec. 19, 2009)	15, 16
<i>Kaufman v. Kaufman</i> , No. 10-P-1143, 2011 WL 1849321 (Mass. App. Ct. May 17, 2011)	34
<i>Kirch v. Embarq Mgmt. Co.</i> , 702 F.3d 1245 (10th Cir. 2012)	23, 26, 30
<i>Kwaak v. Pfizer, Inc.</i> , 71 Mass. App. Ct. 293 (2008)	38, 47

TABLE OF AUTHORITIES
CONTINUED

	Page(s)
<i>L.L. v. Com.</i> , 470 Mass. 169 (2014)	41
<i>Leary v. Contributory Ret. App. Bd.</i> , 421 Mass. 344 (1995)	25
<i>Leocal v. Ashcroft</i> , 543 U.S. 1 (2004)	11
<i>MacNeill Eng'g Co., Inc. v. Trisport, Ltd.</i> , 59 F. Supp. 2d 199 (D. Mass. 1999)	15, 16
<i>Mass. Insurers Insolvency Fund v. Smith</i> , 458 Mass. 561 (2010)	20
<i>Medina v. Cty. of Riverside</i> , 308 F. App'x 118 (9th Cir. 2009)	39
<i>Moelis v. Berkshire Life Ins. Co.</i> , 451 Mass. 483 (2008)	40
<i>Murray v. Fin. Visions, Inc.</i> , No. 07-cv-2578, 2008 WL 4850328 (D. Ariz. Nov. 7, 2008)	38
<i>Nat'l Ass'n of Regulatory Util. Comm'rs v. FCC</i> , 533 F.2d 601 (D.C. Cir. 1976)	28
<i>In re Neurontin Mktg. and Sales Practices Litig.</i> , 244 F.R.D. 89 (D. Mass. 2007)	47
<i>New England Power Co. v. N.H.</i> , 455 U.S. 331 (1982)	20
<i>O'Sullivan v. NYNEX Corp.</i> , 426 Mass. 261 (1997)	passim
<i>Pendell v. AMS/Oil, Inc.</i> , No. 84-cv-4108, 1986 WL 5286 (D. Mass. Apr. 30, 1986)	11, 14, 15, 16

TABLE OF AUTHORITIES
CONTINUED

	Page (s)
<i>People v. Nakai</i> , 183 Cal. App. 4th 499 (2010)	37
<i>Peters v. Equiserve Inc.</i> , No. 05-cv-1052, 2006 WL 709997 (Mass. Super. Ct. Feb. 24, 2006)	27
<i>Pike v. Bruce Church, Inc.</i> , 397 U.S. 137 (1970)	18, 20
<i>Pine v. Rust</i> , 404 Mass. 411 (1989)	12
<i>PSINet, Inc. v. Chapman</i> , 362 F.3d 227 (4th Cir. 2004)	18, 19
<i>Restuccia v. Burk Tech., Inc.</i> , No. CA 952125, 1996 WL 1329386 (Mass. Super. Ct. Aug. 13, 1996)	22, 31
<i>Rubenstein v. Liberty Mut. Ins. Co.</i> , No. 90-cv-1687, 1991 WL 787069 (Mass. Super. Ct. Oct. 3, 1991)	49
<i>S. Cent. Timber Dev., Inc. v. Wunnicke</i> , 467 U.S. 82 (1984)	20
<i>Schrier v. BankNorth, N.A. Mass.</i> , No. 021050B, 2004 WL 3152399 (Mass. Super. Ct. Dec. 30, 2004)	38
<i>Se. Booksellers Ass'n v. McMaster</i> , 371 F. Supp. 2d 773 (D.S.C. 2005)	19
<i>Shanley v. Cadle</i> , 277 F.R.D. 63 (D. Mass. 2011)	45
<i>Shefts v. Petrakis</i> , 758 F. Supp. 2d 620 (C.D. Ill. 2010)	37
<i>Symmons v. O'Keefe</i> , 419 Mass. 288 (1995)	35

TABLE OF AUTHORITIES
CONTINUED

	Page(s)
<i>U.S. v. Footman</i> , 215 F.3d 145 (1st Cir. 2000)	37
<i>U.S. v. Nippon Paper Indus. Co., Ltd.</i> , 109 F.3d 1 (1st Cir. 1997)	11
<i>U.S. v. Thompson/Center Arms Co.</i> , 504 U.S. 505 (1992)	11
<i>In re Vasquez</i> , 428 Mass. 842 (1999)	8
<i>Wal-Mart Stores, Inc. v. Dukes</i> , 131 S. Ct. 2541 (2011)	44
<i>Waters v. EarthLink, Inc.</i> , No. 01-cv-0628, 2006 WL 1549685 (Mass. Super. Ct. May 10, 2006)	46, 47
 Statutes	
M.G.L. c. 272 § 99.....	passim
 Other Authorities	
BLACK'S LAW DICTIONARY (8th Ed. 2004.)	31
Restatement (Second) of Conflict of Laws (1971)	13, 14

ADDENDUM

Page of Addendum

M.G.L.A. c. 272 § 99.....Add. 001

Memorandum And Order On Cross-Motions For Summary
Judgment, *Marquis v. Google Inc.*, No. 11-
2808-BLS1 (Feb. 13, 2015).....Add. 014

Memorandum Of Decision And Order On Plaintiff's
Motion For Class Certification, *Marquis v.*
Google Inc., No. 11-2808-BLS1 (June 19,
2014).....Add. 032

Memorandum Of Decision And Order On Defendant
Google Inc.'s Motion To Dismiss, *Marquis v.*
Google Inc., No. 11-2808-BLS1 (Jan. 17,
2012).....Add. 063

STATEMENT OF THE ISSUES

- I. Did the trial court properly hold that the Wiretap Act, M.G.L. c. 272 § 99(Q) (the "Wiretap Act" or "Act"), does not apply to Google Inc.'s ("Google's") extraterritorial conduct?
- II. Is summary judgment in Google's favor warranted on the additional ground that Google's automated processing of email falls within the "ordinary course of its business" ("OCB") exception to the Act?
- III. Did the trial court properly exercise its discretion in denying class certification because individualized issues of consent predominated over common issues?
- IV. Was class certification properly denied on the additional grounds that Google's alleged "interceptions" cannot be shown on a classwide basis, the class is unascertainable and massively overbroad, and Plaintiff Debra L. Marquis ("Plaintiff") failed to properly raise the issue of a sub-class?
- V. Did the trial court err in denying Google's Motion to Dismiss where the complaint shows that Google's automated processing of email falls within the OCB exception to the Act?

STATEMENT OF THE CASE

I. PRIOR PROCEEDINGS

Google agrees with Plaintiff's history of the proceedings (Pl.-Appellant/Cross-Appellee's Opening Brief ("POB") 3.)

II. STATEMENT OF THE FACTS

A. Google's Gmail Service.

Google launched Gmail in 2004 as a free, web-based email service. (Joint Appendix ("JA") 0007

¶¶ 7-8.) It is now one of the most popular email services in the world, with hundreds of millions of users. Google Apps is a related service in which Google enables businesses and other entities to provide a Gmail-type email service. (JA 0828-29 ¶ 46.)

Like most email service providers, Google applies automated processing to scan email contents for numerous purposes, including detecting spam and computer viruses and allowing users to search their messages and to interact with email content in various ways (like clicking on an address in an email to view a map of the location), among others. (JA 0820-21 ¶¶ 19-21; 1120-21; 1126-27.) Automated scanning also allows Google to show more relevant advertisements in Gmail by automatically scanning the text of emails for key terms and matching those terms to an ad. (JA 0815 ¶ 14.) The revenue from these targeted ads helps offset the cost of providing the free Gmail service. (JA 1083-84 ¶ 2; 1090 ¶ 2; 1092 ¶ 7.) No humans review email for the purposes of serving targeted advertisements. (JA 0815 ¶ 14; 0821 ¶ 22.) Moreover, Google does not share the contents of emails with any third party, including advertisers.¹ (JA 0604-10;

¹ This privacy protection for Gmail users is subject only to narrow exceptions as specifically laid out in Google's Privacy Policy, such as responding to an enforceable government demand. (JA 0604-30.)

0619-24; 0632-34.)

The factual record in this case makes clear that the scanning processes Google uses to provide targeted advertising are not separate from those used to serve other business purposes. For example, one process enables targeted advertising along with various other features, like identifying package tracking information in an email to create a link for users to access the shipping company's website, (JA 0820 ¶ 19), and is also to "improve the spam filtering process in Gmail." (JA 0821 ¶ 21.)

Moreover, the evidence before the trial court showed that Gmail's scanning processes are not applied uniformly to all emails. To the contrary, different features of Gmail's processes apply scanning in different circumstances and are subject to different exceptions based on individual factors that differ from email to email. (JA 0813-24 ¶¶ 5-27.) For example, Google's evidence showed that one of the disputed scanning processes does not apply to many common types of email content, like photos, attachments, and contents in links; and, for a time, it did not apply to emails that were marked as spam. (JA 0822-23 ¶ 25; see also JA 0814-19 ¶¶ 11-17².)

Google has no way to determine if a non-Gmail

² The cited pages set forth additional exceptions to Google's other disputed scanning process.

user's emails were scanned by these processes without accessing the email accounts of each Gmail user who communicated with that individual. (JA 0819 ¶¶ 15-16; 0823-24 ¶ 27.) Even then, it may be impossible to determine if the proposed class member's emails were scanned. (JA 0819 ¶ 16; 0824-25 ¶¶ 30-32; 0829 ¶ 51.)

All of the scanning processes related to targeted advertising are implemented using servers located outside of Massachusetts. (JA 1235 ¶¶ 2-3.)

B. Google's Disclosures Of Its Automated Processing.

To use Gmail, users must affirmatively agree to Google's Terms of Service ("TOS") and its incorporated Privacy Policy, which explain how Google uses data from its users.³ (JA 0523; 0546-50 ¶¶ 9-20; 0599-0631.) Google also discloses in various web pages and other public sources that emails are automatically scanned to show targeted ads and for other purposes. (JA 0551-52; 0558-59; 0562; 0669-71; 0680-81.) These disclosures have been in place throughout the class period. (JA 0550-62 ¶¶ 22-51; 0669-0711.)

Thousands of non-Google sources have also discussed and publicized the automated scanning of

³ For example, Google's 2010 Privacy Policy explains that user data is used to "[p]rovide, maintain, protect, and improve [Google] services (including advertising services) and develop new services. . . ." (JA 0622.)

emails in Gmail since its launch in 2004. (JA 0040-76 ¶¶ 4-78; 0079-459.) The media extensively covered Gmail's launch, with numerous stories focusing on the automated scanning used to serve targeted ads. (*Id.*) In the years since, there have been thousands of stories about Gmail in a variety of media channels. (*Id.*) Notably, the comments posted in the online versions of numerous articles show that many are well aware of Gmail's automated scanning and have no issue with it. (JA 0067-76 ¶ 78.)

In short, there are innumerable ways in which someone could learn of Gmail's automated scanning of emails apart from Google's own disclosures.

C. Google Has No Way Of Identifying Members Of Plaintiff's Proposed Class.

Plaintiff sought certification of a class consisting of Massachusetts residents who are non-Gmail users and whose emails were scanned by Google's automated processes. (POB 28.) As discussed above, absent review of each individual email, Google has no way to determine if a non-Gmail user's emails were scanned. Similarly, Google has no internal data that could be used to reliably identify non-Gmail users who reside in Massachusetts and who communicated with Gmail users during the class period. (JA 0829 ¶ 51.)

SUMMARY OF ARGUMENT

Plaintiff's Appeal:

Summary Judgment: The trial court properly granted summary judgment in Google's favor because (1) the undisputed facts show that the alleged wrongful processing of emails occurs exclusively outside of Massachusetts, and (2) the Act, as a criminal statute, is presumed not to apply to extraterritorial conduct. Plaintiff's effort to single out the civil remedy of the criminal statute for broader application beyond Massachusetts' borders is unavailing and does not allow her to avoid the longstanding presumption against extraterritorial application. (Argument 8-20.)

Plaintiff's claims also fail as a matter of law because it is undisputed that the processing at issue serves legitimate business purposes—providing an additional and alternative basis to affirm the trial court's order. Among other things, Google's processing assists in protecting users from spam and other abuses and enables targeted advertising that generates revenue to support the free Gmail service. These undisputed business purposes bring Google's conduct squarely within the OCB exception of the Act. Plaintiff's main rebuttal—that revenue generation is not a legitimate business purpose—borders on frivolous and underscores her inability to credibly dispute Google's arguments. (*Id.* 20-33.)

Class certification: The trial court did not

abuse its broad discretion in denying class certification. Critically, Plaintiff concedes that an individual would have no claim under the Act if she knew that emails sent to Gmail users are subject to automated processing. The trial court correctly found that this issue is not amenable to classwide treatment because it turns on highly individualized evidence, including an assessment of the myriad disclosures and sources of knowledge reflected in the record below. (*Id.* 36-43.)

Moreover, the denial of certification can also be affirmed on the alternative grounds that (1) Plaintiff offered no feasible method to identify the specific emails that were subject to the alleged wrongful processing, or even to ascertain the proposed class of Massachusetts residents who exchanged emails with Gmail users, and (2) even if this proposed class could be identified, it would include individuals with no claim under Plaintiff's theory of liability, rendering the class impermissibly overbroad. (*Id.* 44-49.)

Google's Cross-Appeal: The trial court erred in denying Google's Motion to Dismiss Plaintiff's Complaint because, on the face of the Complaint, Google's conduct falls within the OCB exception. The trial court should have granted dismissal with prejudice on this basis. (*Id.* 49-50.)

ARGUMENT

III. THE TRIAL COURT PROPERLY GRANTED SUMMARY JUDGMENT DISMISSING PLAINTIFF'S CLAIM.

A. The Act Does Not Apply To Google's Conduct Outside Of Massachusetts.

The trial court correctly held that the Act does not apply to Google's automated processing of emails occurring outside of Massachusetts.⁴

1. The Wiretap Act Is A Criminal Statute Subject To The Presumption Against Extraterritorial Application.

The Wiretap Act is a criminal statute under Part IV of the Massachusetts General Laws entitled "Crimes, Punishments and Proceedings in Criminal Cases." When the Legislature created a civil remedy for unlawful wiretapping, it notably placed it within this criminal statute. As such, the law should be interpreted as a criminal law absent a contrary indication by the Legislature. See *Chin v. Merriot*, 470 Mass. 527, 532 (2015) (in construing statute, the court should "consider also other sections of the statute, and examine the pertinent language in the context of the entire statute."); *Com. v. Graham*, 388 Mass. 115, 120 (1983) ("the title [of an act] may be used for the purpose of ascertaining its proper limitations.").

As a criminal statute, the terms of the Act are

⁴ Plaintiff does not dispute that Google's automated processing occurs outside of Massachusetts. (JA 1065 ¶ 16.)

subject to the longstanding presumption against extraterritorial application.⁵ *In re Vasquez*, 428 Mass. 842, 848 (1999) (rule against extraterritorial application of criminal laws is "axiomatic"); *Armstrong*, 73 Mass. App. Ct. at 249. Indeed, Massachusetts courts applying this rule have uniformly held that the Act does not apply to interceptions outside of Massachusetts. *Com. v. Wilcox*, 63 Mass. App. Ct. 131, 139 (2005) (holding that the Act did not apply to a recording in Rhode Island and noting that the party seeking to invoke the Act was unable to cite any "authority for the proposition that [the Act] applies to recordings made outside of Massachusetts."); *Com. v. Tibbs*, No. 01-cr-10170, 2007 WL 4644818, at *4 (Mass. Super. Ct. Jan. 4, 2008) ("A

⁵ Plaintiff does not argue on appeal that the "effects doctrine"—the exception to the general rule against extraterritorial application of a criminal statute—applies in this case, and the trial court affirmatively held that it did not apply. (JA 1669.) In order for the "effects doctrine" to apply here, at least some part of the criminal act must touch the Commonwealth. It does not. See *Com. v. Armstrong*, 73 Mass. App. Ct. 245, 249-50 (2008) (effects doctrine did not apply where no predicate acts in furtherance of the crime occurred in Massachusetts). Moreover, Google must have had actual intent to produce a negative effect in Massachusetts. *Com. v. Fafone*, 416 Mass. 329, 331 (1993) (setting aside verdict where there was no evidence the defendant knew drugs would be distributed in Massachusetts). It is undisputed that Google cannot reliably determine whether Gmail users or non-users "reside" in Massachusetts and, therefore, Google could not have such actual intent. (JA 0829-30 ¶¶ 51-52.)

conversation recorded in Rhode Island with only one party's consent does not violate [the Act], because the statute does not apply to recordings made outside of Massachusetts.") (citation and quotation omitted); *Com. v. Maccini*, No. 06-cr-0873, 2007 WL 1203560, at *2 (Mass. Super. Ct. Apr. 23, 2007) (finding the Act did not apply to interception in Ohio because "nothing in the [Act] suggests any intention to regulate conduct outside the bounds of the Commonwealth").

The fact that this case involves the civil remedy of the Wiretap Act does not mandate a different result, as Plaintiff contends.⁶ As an initial matter, Plaintiff cites no statutory language or legislative history suggesting that the Legislature intended the Act's civil remedy to apply extraterritorially. This is telling because the Legislature is presumed to have known of the longstanding rule against extraterritorial application when it included a civil remedy in the criminal law. *Com. v. Vega*, 449 Mass. 227, 231-32 (2007) ("The Legislature is presumed to be aware of the prior state of the law as explicated by the decisions of this court.") (citation omitted). Yet the Legislature gave no indication that this civil remedy should have greater reach than the criminal portions of the same statute. To the contrary, the

⁶ Plaintiff concedes the Act's criminal sections do not apply to Google's extraterritorial conduct. (POB 9.)

Preamble to the Act repeatedly emphasizes that the Act, as a whole, addresses conduct "within the commonwealth," indicating that the law's purpose is to regulate in-state conduct only. See also *Pendell v. AMS/Oil, Inc.*, No. 84-cv-4108, 1986 WL 5286, at *4 (D. Mass. Apr. 30, 1986) ("There is no language whatsoever to indicate that the [Wiretap Act] was intended to be given extraterritorial effect.").

In analogous contexts involving statutes with both civil and criminal aspects, the Supreme Court has held that the law must be interpreted consistently with its criminal applications. Thus, the rule of lenity—traditionally applied only in the context of criminal statutes—also applies to a civil statute with criminal applications. *Crandon v. U.S.*, 494 U.S. 152, 158 (1990); see also *U.S. v. Thompson/Center Arms Co.*, 504 U.S. 505, 517-18 (1992); *Leocal v. Ashcroft*, 543 U.S. 1, 12 n.8 (2004) ("we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context.") (citation omitted). The First Circuit has similarly held that "common sense suggests that courts should interpret the same language in the same section of the same statute uniformly, regardless of whether the impetus for interpretation is criminal or civil." *U.S. v. Nippon Paper Indus. Co., Ltd.*, 109 F.3d 1, 4 (1st Cir. 1997). These established principles confirm that the

presumption against extraterritorial conduct should be applied uniformly to the criminal and civil parts of the Act.

The single case Plaintiff cites for the opposite conclusion—*Pine v. Rust*, 404 Mass. 411 (1989)—says nothing about the extraterritorial reach of the Wiretap Act. *Pine* focused on whether the civil remedy requires that the conduct at issue be done “wilfully,”—as required for a criminal violation of the Act—though Section 99(Q) included no similar requirement. *Id.* at 414. Because the provision authorizing a civil remedy does not require willfulness, the court in *Pine* refused to apply the criminal mens rea requirement in the civil context. *Id.* Plaintiff here, in contrast, seeks to expand the scope of a provision of the Act that applies *equally* to the civil and criminal aspects of the law. Moreover, as discussed below (Section II.A.3.), because Plaintiff’s interpretation of the Act would implicate significant constitutional concerns regarding Massachusetts’ ability to regulate out-of-state commerce, the Court should reject it. *Baird v. Attorney Gen.*, 371 Mass. 741, 745 (1977) (“we have regarded the presence of a serious constitutional question under one interpretation of a statute to be a strong indication that a different possible interpretation of that state should be adopted, if the

constitutional issue can be avoided thereby.") (citations omitted).

2. Choice-Of-Law Principles Confirm That The Wiretap Act Does Not Apply Here.

The trial court's ruling should also be affirmed under choice-of-law principles. Massachusetts applies a "functional" choice-of-law analysis that "responds to the interests of the parties, the States involved, and the interstate system as a whole." *Bushkin Assocs., Inc. v. Raytheon Co.*, 393 Mass. 622, 631 (1985). In applying this test, courts look first to the section of the Restatement (Second) of Conflict of Laws ("Restatement") most analogous to the conduct at issue, and, thereafter, assess whether the outcome under that section is appropriate in light of "the choice-influencing factors listed in § 6(2) of the Restatement." *Id.* at 634. Plaintiff argues that this case should be governed by Section 152 of the Restatement, which deals with invasion of privacy rights, and that this section mandates application of Massachusetts' law. Plaintiff fails, however, to take the mandatory next step and apply Section 6 of the Restatement. (POB 10-11.) Regardless of the outcome of the analysis under Section 152, Section 6 of the Restatement counsels against applying the Wiretap Act to Google's extraterritorial conduct.

[T]he factors relevant to the choice of the

applicable rule of law include (a) the needs of the interstate and international systems, (b) the relevant policies of the forum, (c) the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue, (d) the protection of justified expectations, (e) the basic policies underlying the particular field of law, (f) certainty, predictability and uniformity of result, and (g) ease in the determination and application of the law to be applied."

The Restatement states that it is "[p]robably the most important function of choice-of-law rules . . . to make the interstate and international systems work well." Restatement § 6 cmt. D (1971).

Pendell is particularly instructive here because it applied the choice-of-law analysis above and found that Massachusetts law should not apply to interception outside of the Commonwealth. 1986 WL 5286, at *3-5. In *Pendell*, the court asked whether the law of Massachusetts or Rhode Island should apply to the defendant's alleged "interception" under the Wiretap Act. *Id.* Because the defendant, a resident of Rhode Island, had consented to the recording of the communication at issue, he had not violated Rhode Island's wiretap statute but could still have been liable if Massachusetts' Act applied. *Id.*

The *Pendell* court found that the interests of the parties and the interests of the respective states

were relatively comparable.⁷ *Id.* at *3. However, it found that the interests of the interstate system weighed in favor of rejecting the application of Massachusetts law because the effect of such application would be to regulate the defendant's conduct outside the Commonwealth. *Id.* The court held that "[c]onsidering the interstate system as a whole, the better rule is that a local statute should not be given extraterritorial effect so as to regulate conduct in another jurisdiction." *Id.* at *4; see also *MacNeill Eng'g Co., Inc. v. Trisport, Ltd.*, 59 F. Supp. 2d 199, 202 (D. Mass. 1999) (following *Pendell* and finding that the Act did not apply to an interception outside the Commonwealth).

As noted by the trial court, and discussed in Section II.A.3. herein, application of the Act in this case would effectively regulate Google's conduct outside of the Commonwealth. Accordingly, as in *Pendell* and *MacNeill*, the Wiretap Act should not apply

⁷ As to the interests of the parties, while the plaintiff could have reasonably expected to be afforded the protection of the Act, the defendant also could have reasonably expected that he would not be subject to liability for conduct that was legal in his home state. As to the interests of the States involved, the court recognized that both states "ha[d] a significant interest both in regulating their respective citizens' conduct within their own borders and in protecting their citizens' rights . . . [and] [n]either state's interest could be said to supercede [sic] that of the other" *Pendell*, 1986 WL 5286, at *4.

to Google's extraterritorial conduct.

Plaintiff relies on *Heffernan v. Hashampour*, No. 09-cv-2060, 2009 WL 6361870, at *3 n.6 (Mass. Super. Ct. Dec. 19, 2009) to support a different result, but the *Heffernan* court did not even consider the effects of the application of the Wiretap Act on the interstate system, as required under the applicable choice-of-law analysis. Plaintiff further argues that the trial court erred in relying on *Pendell* and *MacNeill* because those cases purportedly applied the wrong choice-of-law test (the *lex loci delicti* doctrine). Plaintiff's interpretation of these cases is incorrect and misleading. In *Pendell*, the court briefly discussed whether to apply the *lex loci delicti* doctrine, but went on to say that "[t]he issue . . . need not be decided." 1986 WL 5286 at *3 (emphasis added). Instead, the court analyzed the choice-of-law issue under the "more pragmatic and functional approach" in *Bushkin*—the same test applied by Plaintiff's own cited authorities. *Id.*

3. Extraterritorial Application Of The Act Would Violate The Dormant Commerce Clause.

A state statute that has extraterritorial reach, whether intended or not, is a per se violation of the Dormant Commerce Clause ("DCC"). *Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989) (holding that when a state

statute regulates commerce occurring wholly outside the state's borders or when it has a "practical effect" of controlling conduct outside of the state, the statute will be invalid under the DCC). Plaintiff does not dispute that the automated processing she challenges occurred outside of Massachusetts. (JA 1065 ¶ 16.) Moreover, she recognizes 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." (POB 13)(citing *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 573 (1996)). She claims, however, that, because she seeks to apply the Act only to violations "against Massachusetts residents," there is no DCC problem. [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] (JA 0829-30 ¶¶ 51-52.) Take, for example, an email sent by a Gmail user from Rhode Island (which allows scanning based on the consent of a single party) to a group of ten recipients also in Rhode Island, which is then scanned by Google servers located in another state. Under Plaintiff's theory, Massachusetts law would still govern the scanning of that communication if a single Massachusetts resident were copied on the message, [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

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.

(JA 1668 (emphasis in original).) A number of other courts have found that state laws placed an excessive burden on interstate commerce by attempting to regulate Internet activity because, as here, there is no feasible way to discern the geographic location of the conduct at issue. *PSINet*, 362 F.3d at 240 (state statute imposed excessive burden on interstate commerce); *Am. Civil Liberties Union v. Johnson*, 194 F.3d 1149, 1161 (10th Cir. 1999) (same); *Se. Booksellers Ass'n v. McMaster*, 371 F. Supp. 2d 773 (D.S.C. 2005) (same). Indeed, if the Wiretap Act were applied to Google's conduct, Massachusetts would essentially impose a two-party consent regime on the entire nation.⁸ This excessive burden outweighs the local benefits of the Act and, therefore, fails the *Pike* test.

Plaintiff seeks to avoid the DCC by pointing out that the federal wiretap statute does not expressly

⁸ As the federal wiretap law is a one-party consent regime, applying the Act to Google's extraterritorial conduct would effectively preempt federal law.

preempt the Act. (See POB 13-15.) But that is not the test for evaluating whether the DCC applies. Rather, "for a state regulation to be removed from the reach of the dormant Commerce Clause, congressional intent must be *unmistakably clear*." *S. Cent. Timber Dev., Inc. v. Wunnicke*, 467 U.S. 82, 91-92 (1984) (emphasis added). This stringent standard is not met where, as here, "Congress did no more than leave standing whatever valid state laws then existed relating to" the subject matter of the federal law. *New England Power Co. v. N.H.*, 455 U.S. 331, 341 (1982). Statutes that "simply save[] from pre-emption" pre-existing state laws do not "evinced[] a congressional intent to alter the limits of state power otherwise imposed by the Commerce Clause." *Id.*

B. Alternative Bases For Affirming The Trial Court's Summary Judgment Decision.

1. The OCB Exception.

While the trial court did not rule on the OCB exception, the Court can nonetheless affirm the summary judgment order on that basis. *Mass. Insurers Insolvency Fund v. Smith*, 458 Mass. 561, 564 (2010).

a. The OCB Exception Applies Because Google's Automated Scanning Has A Legitimate Business Purpose.

A Wiretap Act claim requires the use of an "intercepting device," which *excludes* any "instrument, equipment, facility, or a component thereof . . .

being used by a communications common carrier in the ordinary course of its business." M.G.L. c. 272 § 99(B)(3). The Supreme Judicial Court ("SJC") has held that this exception applies broadly to **any practice** supported by a "legitimate business purpose." *O'Sullivan v. NYNEX Corp.*, 426 Mass. 261, 266-67 (1997); *Dillon v. Mass. Bay Transp. Auth.*, 49 Mass. App. Ct. 309, 319 (2000) (relying on *O'Sullivan* to hold that "[o]rdinary course of . . . business' translates as 'legitimate business purpose.'")

In *O'Sullivan*, the SJC held the defendant could not be liable for recording customer calls because it did so for the business purposes of monitoring the quality of its marketing calls, complying with statutory guidelines, and training its employees. *O'Sullivan*, 426 Mass. at 266-67; see also *Dillon*, 49 Mass. App. Ct. at 319 (dismissing Wiretap Act claim where defendant's call recording policy was supported by "considerations of efficiency, safety, and sound maintenance record-keeping"). Given those business purposes, the *O'Sullivan* court explained that the defendant could not be liable even though its customers received no notice of the recording.⁹

⁹ See also, *Crosland v. Horgan*, 401 Mass. 271, 274 (1987) ("ordinary course of business" applied where a police detective asked an employee to listen to a call between two other employees on their employer's phone system); *Gilday v. Dubois*, 124 F.3d 277, 290 (1st Cir. 1997) (holding under Massachusetts law that automated

O'Sullivan, 426 Mass. at 262.

Federal cases construing the parallel provision of the federal wiretap act further clarify the broad scope of the OCB exception.¹⁰ In fact, the federal exception has been applied specifically to the Google practices at issue here. *In re Google, Inc. Privacy Policy Litigation*, No. 12-cv-1382, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012), involved a claim alleging that "an interception occurred when [plaintiffs'] content from one Google product was . . . combined with information from another Google product that also was stored on Google's servers." *Id.* at *5-6. These claims were far broader than here; plaintiffs alleged that Google improperly accesses information from dozens of Google products, including Gmail, without consent. The court held that the OCB exception precluded any liability because "[a]n interception claim . . . requires the use of a defined 'device,'

"call detailing" of calls placed from a prison was in the ordinary course of the company's business); *Restuccia v. Burk Tech., Inc.*, No. CA 952125, 1996 WL 1329386, at *2 (Mass. Super. Ct. Aug. 13, 1996) (applying related exception under the Act and holding that a "back-up system which automatically stores all computer files including plaintiffs' E-Mail messages" was within the "ordinary course of business").

¹⁰ Cases applying the federal version of the OCB exception are highly persuasive authority. *O'Sullivan*, 426 Mass. at 264 & n.5 ("[W]e shall construe the Massachusetts statute in accordance with the construction given the cognate Federal statute by the Federal courts.").

which cannot include Google's own systems"
Id. at *5 (emphasis added). As the court explained,
the federal wiretap act "excludes from the definition
of a 'device' a provider's own equipment used in the
ordinary course of business." *Id.* at *6. Because the
complaint did not allege any "device" beyond Google's
own systems, and because the alleged acts were
implemented for the business purpose of providing
Google's services, the court dismissed the claim. *Id.*

Other federal courts have applied the OCB
exception to practices similar to those alleged here.
Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1245-48
(10th Cir. 2012) (affirming dismissal of wiretap claim
where ISP's "interception" of plaintiffs' browsing
histories to deliver targeted advertising was in OCB);
Hall v. EarthLink Network, Inc., 396 F.3d 500, 505 (2d
Cir. 2005) (affirming dismissal of wiretap claim
because ISP's "routers, servers and other computer
equipment" used to process emails were used in OCB).¹¹

¹¹ While these federal cases are consistent with
Massachusetts law, the court in *In re Google Inc.
Gmail Litigation*, No. 13-md-2430, 2013 WL 5423918
(N.D. Cal. Sept. 26, 2013) ("Gmail MDL") applied a
different standard that conflicts with *O'Sullivan*
because it is not based on a "legitimate business
purpose" standard. Moreover, the court emphasized
that its ruling was based on the pleadings and further
"factual development would be necessary in determining
whether Google's interceptions fall within the
'ordinary course of business' exception." Order Den.
Defs.' Mot. for § 1292(b) Certification for
Interlocutory Review at 6 n.2, *Gmail MDL*, No. 13-md-

The practices here fall squarely within the OCB exception for similar reasons. The undisputed evidence shows that Google scans emails—not to conduct “secret” surveillance or for any other reason barred by the Act—but for the “legitimate business purpose” of providing a feature-rich email service to its users. (JA 0006-07 ¶¶ 2, 8-9; 1090 ¶ 2; 1092 ¶ 7; 1155-58; 1229-33); *O’Sullivan*, 426 Mass. at 266-67. Because the alleged “interceptions” consist solely of Google’s standard practices in providing the Gmail service and are implemented using Google’s normal systems in the ordinary course of business, Plaintiff’s claims were properly dismissed as a matter of law. See *Hall*, 396 F.3d at 505; *In re Google Privacy Policy*, 2012 WL 6738343, at *5.

Indeed, Plaintiff acknowledges that the specific practice she seeks to challenge—the automated scanning of emails to display targeted advertising—is part of Google’s ordinary business. Plaintiff admits that Google applies automated scanning to “direct targeted advertising *for its own business.*” (JA 1308 (emphasis added).) Moreover, Plaintiff concedes that Gmail users consent to scanning by agreeing to Google’s TOS and Privacy Policy by limiting her class to non-Gmail

2430 (N.D. Cal. Jan. 27, 2014), ECF No. 129. The motion to dismiss order in the *Gmail MDL* thus has no precedential value here.

users only. (POB 28.) The Court need look no further than these admissions to apply the OCB exception and affirm the grant of summary judgment.

b. The OCB Exception Is Not Limited To The Employer-Employee Context.

Plaintiff claims the OCB exception is limited to the recording of employee communications, (POB 16-17), but this argument fails for multiple reasons.

First, this artificial limitation appears nowhere in the statute. See *Comm'r of Correction v. Super. Ct. Dept. Cty. of Worcester*, 446 Mass. 123, 126 (2006) ("We do not read into the statute a provision which the Legislature did not see fit to put there"). Indeed, the Legislature used the term "employee" in other sections of the Act (e.g., M.G.L. c. 272, § 99(B)(13)), confirming that its omission from the OCB exception was purposeful. See *Leary v. Contributory Ret. App. Bd.*, 421 Mass. 344, 348 (1995) ("[W]hen the Legislature has employed specific language in one part of a statute, but not in another part which deals with the same topic, the earlier language should not be implied where it is not present.") (citations omitted).

Second, the *O'Sullivan* case says only that "[m]ost cases that have discussed whether an interception is 'within the ordinary course of business' involved situations where an employer was

monitoring employee conversations." 426 Mass. at 266 (citations omitted). The court did not hold that the exception applies *only* in the employer/employee context.¹² Indeed, courts have readily applied the exception outside of the employer-employee context.¹³ See *Crosland*, 401 Mass. at 274; *Gilday*, 124 F.3d at 290; *Kirch*, 702 F.3d at 1245-48; *Hall*, 396 F.3d at 505.

Third, Plaintiff's "employee communications" limitation would cripple the normal operation of email services that depend on automated scanning for various purposes beyond the employee context. For example, email service providers could no longer apply scanning to detect spam and to prevent viruses in emails because such scanning does not involve employee communications and would thus fall beyond the scope of the exception as Plaintiff conceives it.¹⁴ The Court

¹² *O'Sullivan* went on to hold that the "general rule" in *employer/employee* cases is that "eavesdropping on [an employee's] private calls is illegal unless there 'is a legitimate business purpose.'" 426 Mass. at 266. Even if this rule applied outside of the employer/employee context, Google *does* have a legitimate business purpose, as discussed above.

¹³ Contrary to Plaintiff's assertion, this Court may consider the cases cited by Google regarding the OCB exception in the employer/employee context. This Court reviews questions of law *de novo* and is not bound by Judge Lauriat's incorrect pronouncement at the motion to dismiss stage that Google could not rely on these cases.

¹⁴ Plaintiff's position would also outlaw any number of other commonplace email services like user-directed

should not endorse this absurd outcome.

c. **The Communications Common Carrier Element Does Not Bar Google From Invoking The OCB Exception.**

Plaintiff further argues the OCB exception does not apply because Google is not a "communications common carrier." (POB 18-19.) This narrow interpretation of the OCB exception ignores governing law holding that this provision must be applied flexibly based on "the reality of the telecommunications industry as it exists today, not as it existed two decades ago." *Dillon*, 49 Mass. App. Ct. at 316; see also *id.* at 315 (the OCB exception should be applied broadly "to preserve it in its intrinsic intended scope and maintain its viability in the broad run of cases"); *Peters v. Equiserve Inc.*, No. 05-cv-1052, 2006 WL 709997, at *5 (Mass. Super. Ct. Feb. 24, 2006) (applying the OCB exception to a financial services company that did not provide communication services). Thus, the relevant inquiry is whether the Gmail service is functionally similar, at least in part, to the "services [that were] earlier . . . provided by a telephone company" when the Act was enacted. *Dillon*, 49 Mass. App. Ct. at 314. Gmail

filtering, indexing emails for search, and identifying package tracking information, all of which depend on automated scanning. (JA 0820-21 ¶¶ 19-21; 1119-23; 1124-38.)

plainly meets this requirement because it provides to the public a means of sending and receiving communications. See *Nat'l Ass'n of Regulatory Util. Comm'rs v. FCC*, 533 F.2d 601, 608 (D.C. Cir. 1976) (explaining that the definition of a "common carrier" is based primarily on "a quasi-public character, which arises out of the undertaking to carry for all people indifferently") (quotation and citations omitted).

Plaintiff's comparison of supposedly "non-common" carriers Google and Yahoo, and "common carriers" Verizon and Comcast, highlights the absurdity of her interpretation. Verizon and Comcast also provide web-based email services, similar to Gmail. (JA 1512-17.) Under Plaintiff's theory, Verizon and Comcast are entitled to scan emails that a Gmail user sends to Verizon/Comcast users, but Google is barred from applying the same scanning when those Verizon/Comcast users reply to the Gmail user. The Legislature could not have intended this bizarre result.¹⁵

Because the trial court found that the Act's

¹⁵ Plaintiff has abandoned on appeal her argument that Google does not qualify for the OCB exception because it does not use "telephone or telegraph instrument, equipment, facility, or a component thereof." M.G.L. c. 272 § 99(B)(3). Were the Court to consider this issue, that provision does not preclude Google from invoking the OCB exception. See *Hall*, 396 F.3d at 504-05 (applying OCB exception to ISP regardless of "telephone or telegraph" requirement); see also *In re Google Privacy Policy*, 2012 WL 6738343, at *5 (same).

liability provisions apply to email service providers, it is necessary to apply the exceptions to liability (including the OCB exception) in equivalent fashion to harmonize the statute as a whole. Any other outcome would create a contradiction within the statute that would be inherently unfair to Google.¹⁶ *Adams v. City of Bos.*, 461 Mass. 602, 613 (2012) ("Seemingly contradictory provisions of a statute must be harmonized so that the enactment as a whole can effectuate the presumed intent of the Legislature.") (citation and quotation omitted).

d. Plaintiff Fails To Show That Google's Automated Scanning Is Not A "Legitimate Business Purpose."

Plaintiff makes a series of scattershot arguments claiming that Google's automated processing is not supported by a legitimate business purpose, but these arguments all fail.

First, Plaintiff claims that Google is barred from "raising revenue from intercepted communications." (POB 19.) But providing a free service supported by ad revenue is undoubtedly a "legitimate business practice." See *Kirch*, 702 F.3d at 1245-48 (holding that the OCB exception applies to

¹⁶ If the Court declines to apply the OCB exception to Google as a provider of an email service, it should also revisit the question of whether the Act properly applies to emails at all.

the scanning of user data to deliver targeted advertising). The revenue from targeted advertising is precisely what allows Google to provide Gmail as a free service to millions of users. Under Plaintiff's theory, the viability of most Internet services would be cast in doubt, since the basic business model of the Internet often involves a *quid pro quo* in which users receive free services in exchange for receiving paid advertising targeted to their interests (not unlike the decades-old business model of broadcast television). (See JA 1260-61 ¶ 14 (confirming the common industry practice of providing free email service supported by advertising); 1090 ¶ 2; 1092 ¶ 7; 1229-33; 1274-79.) Plaintiff's claims require the Court to make the unprecedented finding that this widespread business model lacks a "legitimate business purpose."¹⁷

Second, it would be absurd to interpret the term "ordinary course of business" as excluding services that generate profits, when profits are a fundamental underlying purpose of most business services. Indeed, "business" is defined as "[a] commercial enterprise carried on for profit." BLACK'S LAW DICTIONARY (8th Ed.

¹⁷ Further, the undisputed evidence shows that Google uses the same processes in connection with *both* spam detection and targeted advertising, underscoring the overall business purposes served by Google's processing. (JA 0821 ¶ 21.)

2004.) The fact that Google generates revenue from targeted ads hardly distinguishes this case from other circumstances where courts have applied the OCB exception. For example, the monitoring of customer service calls in *O'Sullivan* and the backing-up of emails in *Restuccia*, 1996 WL 1329386, at *2, were not done for purely charitable purposes divorced from normal business imperatives. Rather, offering quality customer service and maintaining accurate records enhanced the services—and ultimately the profits—of the businesses in those cases. The automated scanning at issue here is no different.

And even if the OCB exception requires a customer-oriented purpose beyond revenue generation, Google has provided undisputed evidence to this effect. In particular, Google's automated scanning allows it to serve advertisements that are more likely to be interesting to users, rather than bombarding them with irrelevant ads.¹⁸ (JA 1090-92 ¶¶ 3-9; 1099 ¶ 14; 1105 ¶¶ 22-23; 0587-88; 1229-33.) Plaintiff has

¹⁸ Plaintiff appears to limit her claims to Google's scanning for the purposes of ad targeting. (See JA 1315 ("Google 'reads' the content of emails for its own fiscal gain separate and apart from any scanning done for the purposes of ensuring network security and reliability, such as by scanning for viruses and/or spam.")) However, to the extent she is seeking to attack scanning for other purposes, those functions are also supported by legitimate business purposes and provide benefits to users. (See JA 1104-05 ¶¶ 19-21; 1124-38.)

not offered any evidence to refute this business purpose that goes beyond the generation of revenue.

Third, Plaintiff mischaracterizes Google's use of information obtained through scanning, claiming that Google "sell[s] the information contained in Plaintiff's emails." (POB 20.) To be clear, Google does not "sell" user information; it allows advertisers to anonymously target ads to Gmail users who are more likely to be interested in those ads based on words and phrases in the user's emails. Plaintiff offers no evidence to support her false characterization of Google's business model.¹⁹

Fourth, Plaintiff argues Google can "only be exempt if [scanning is] necessary to the safe and secure operation of the system, not as an end in itself." (POB 19.) But this limitation appears nowhere in the Act, and the Court can reject this argument based on a cursory review of the statute. Indeed, the case law confirms there is no such limitation. See *Dillon*, 49 Mass. App. Ct. at 319 (finding call monitoring to be a legitimate business

¹⁹ Even if Google did "sell" these words and phrases, Plaintiff has offered no support for her argument that she has a "property interest" in these words and phrases. (POB 19-20.) And even if she did, a purported violation of a property interest does not automatically result in a Wiretap Act violation, as Plaintiff suggests. To the contrary, Google's conduct would still be subject to the OCB exception.

purpose without asking whether it was "necessary" to the MBTA's operation of its transportation systems); *Hall*, 396 F.3d at 505 (finding email service provider's delivery of emails to closed accounts to be within the ordinary course of its business without asking whether it was a "necessary" practice).²⁰

Fifth, Plaintiff claims that "most" email service providers "do not rely upon" targeted advertising based on automated scanning. (POB 21.) But this is irrelevant. Nothing in the Act suggests the Legislature intended to deprive a company of the OCB exception simply because it chooses to run its business differently (and potentially better) than its competitors. Even if prevailing industry practices were relevant, several major webmail providers generate revenue and support their free services by showing advertising in the user interface, just as Google does in Gmail. (JA 1276-79 ¶¶ 49-55.)

2. The Court Did Not Err In Denying Partial Summary Judgment For Plaintiff.

To prevail on summary judgment, Plaintiff must

²⁰ To the extent Plaintiff's interpretation rests on the "necessary incident" language contained elsewhere in the statute, this would violate the canon of statutory construction that language used in one section should not be imported into another. *Boone v. Commerce Ins. Co.*, 451 Mass. 192, 196-97 (2008). The Legislature knew how and when to incorporate a "necessity" requirement and did not modify the OCB exception in that way. *Id.*

demonstrate that there are no disputed issues of fact as to any of the "essential elements" of her claim. *Kaufman v. Kaufman*, No. 10-P-1143, 2011 WL 1849321, at *2 (Mass. App. Ct. May 17, 2011). To meet this burden, Plaintiff must point to specific evidence to support the elements of her claim. See *Dillon v. Mass. Bay Transp. Auth.*, No. 96-cv-4871, 1998 WL 128998, at *2 (Mass. Super. Ct. Mar. 19, 1998) (citing Mass. R. Civ. P. 56(c)).

Plaintiff failed to present any proof that Google's automated scanning was applied to her emails. As discussed in Section IV.D.1, there are numerous instances in which emails are *not* scanned. (JA 1097-112 ¶¶ 5-45; 1119-20; 1506-11; 1602-03; 1428-30; 1434-37; 1441-42; 1600-01.) To obtain judgment as a matter of law, Plaintiff must present undisputed evidence that her emails were in fact scanned, which necessarily requires her to show whether the multiple exceptions to scanning applied to the specific emails she exchanged with Gmail users. Yet at summary judgment, Plaintiff failed to even *assert*, let alone offer any evidence, that her emails were scanned.

Plaintiff further failed to present any evidence to show that the scanning of her emails—if any—was applied to the *contents* of her emails, as required by M.G.L. c. 272, § 99(B)(4). In fact, Plaintiff refused during discovery to produce the body of her emails

with Gmail users, instead producing only a list of email header information. By providing her email in redacted form, Plaintiff has prevented Google and this Court from assessing whether the "contents" of her email were actually scanned.²¹ Plaintiff's total lack of evidentiary support for the essential elements of her claim precludes judgment as a matter of law.²²

Moreover, whether Plaintiff knew of, and impliedly consented to, Google's automated scanning cannot be resolved on summary judgment. "[W]here a party's state of mind . . . is in issue, summary judgment is disfavored." *G.S. Enters., Inc. v. Falmouth Marine, Inc.*, 410 Mass. 262, 276 n.4 (1991) (quotation and citation omitted). Because "[m]uch depends on the credibility of the witnesses testifying as to their own states of mind . . . the jury should be given an opportunity to observe the demeanor,

²¹ Scanning of the email information provided by Plaintiff—"to," "from," "date," etc.—is not a violation of the Act. This "header information" is critical to email delivery because, among other things, there would be no way to deliver an email without identifying the recipient, or to apply common spam filters based on the sender's information. Scanning of this "header information" is thus part of Google's "ordinary course of business" and excepted from the Act. See M.G.L. c. 272, § 99(B)(3).

²² Plaintiff's failure to show that the contents of her email were "intercepted" provides an additional basis to affirm the grant of summary judgment in Google's favor because Plaintiff has "no reasonable expectation of proving [this] essential element of [her] case" based on any evidence in the record. *Symmons v. O'Keefe*, 419 Mass. 288, 293 (1995) (citations omitted).

during direct and cross-examination, of the witnesses whose states of mind are at issue." *Flesner v. Tech. Commc'ns Corp.*, 410 Mass. 805, 809 (1991) (quotation and citation omitted). Here, as in *Flesner*, a jury should have the opportunity to evaluate Plaintiff's testimony to determine whether she impliedly consented to Google's automated scanning.²³

IV. THE TRIAL COURT PROPERLY DENIED PLAINTIFF'S MOTION FOR CLASS CERTIFICATION.

A. Individuals Who Impliedly Consent To Google's Automated Scanning Have No Claim.

Under established law, an individual who uses a means of communication knowing the communication can be intercepted impliedly consents to the interception and has no claim under the Wiretap Act. While "actual knowledge" is required, a court may look to "objective manifestations of knowledge" that "allow an inference of knowledge." *Com. v. Jackson*, 370 Mass. 502, 507 (1976). Thus, courts must "look to the [claimant's] words and conduct to determine if a conversation is being intercepted unbeknown to him." *Id.*; see also *Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990) (explaining, in the context of the federal

²³ Plaintiff claims that Google "concedes" that she was unaware of Google's automated scanning prior to July 2011. (POB 23.) This is incorrect. At summary judgment, Google conceded only that Plaintiff testified as such in deposition. (JA 0976.) As the only evidence of Plaintiff's knowledge of Google's scanning is her own deposition testimony, the trier of fact should be permitted to evaluate this testimony.

wiretap statute, that "implied consent" depends on "'the circumstances prevailing' in a given situation" and "[t]he circumstances relevant to an implication of consent will vary from case to case" (citation omitted).

The evidence potentially relevant to implied consent is inherently individualized and can include, for example, (1) whether an individual saw a written disclosure of the disputed practice, *U.S. v. Footman*, 215 F.3d 145, 154 (1st Cir. 2000); (2) whether an individual received a verbal explanation, *Griggs-Ryan*, 904 F.2d at 117-19; (3) whether an individual was aware of online privacy policies regarding the disputed practices, see *People v. Nakai*, 183 Cal. App. 4th 499, 518 (2010); (4) whether an individual was familiar with the disputed practices based on the circumstances of his or her employment, see *Shefts v. Petrakis*, 758 F. Supp. 2d 620, 631 (C.D. Ill. 2010); and (5) whether an individual was aware of general industry practices involving email, see, e.g., *Maccini*, 2007 WL 1203560, at *3.²⁴

²⁴ *Campiti v. Walonis*, 611 F.2d 387 (1st Cir. 1979) does not hold differently. That case properly applied the *Jackson* "actual knowledge" standard where there were no "clear and unequivocal objective manifestations of knowledge" because there was no evidence that the plaintiff had any idea—or even speculated—that he was being recorded. The defendant's only argument was that plaintiff "**should**

B. The Trial Court Properly Held That The Issue Of Implied Consent Is Individualized.

Given this established law, the trial court properly held that resolving each claimant's knowledge of automated scanning would require a highly individualized inquiry that cannot be litigated on a classwide basis. (JA 0960-62.) This ruling is in accord with many Massachusetts and federal courts that have denied certification in similar circumstances. *Kwaak v. Pfizer, Inc.*, 71 Mass. App. Ct. 293, 300-02 (2008) (denying certification of consumer fraud claim where some class members would have seen advertisements that were "adequately informative for any reasonable consumer"); *Schrier v. BankNorth, N.A. Mass.*, No. 021050B, 2004 WL 3152399, at *7 (Mass. Super. Ct. Dec. 30, 2004) (denying certification of consumer claim alleging that bank failed to inform customers of higher interest rates, where the defendant "did inform customers, in a variety of ways . . . that it was introducing a new package with competitive interest rates").²⁵

have known his call would probably be monitored" because he was an inmate. *Id.* at 393 (emphasis added).

²⁵ See also, e.g., *Murray v. Fin. Visions, Inc.*, No. 07-cv-2578, 2008 WL 4850328, at *4 (D. Ariz. Nov. 7, 2008) ("defendants' liability under the Wiretap Act will require an individualized showing of each class member's knowledge and consent with respect to each intercepted email."); *Medina v. Cty. of Riverside*, 308 F. App'x 118, 120 (9th Cir. 2009) (affirming denial of certification of a class of prisoners who claimed that

In re Google Inc. Gmail Litigation, 13-md-2430, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014) ("*Gmail*") is particularly instructive. *Gmail* involved a claim alleging that the very same automated processing at issue here violated state and federal wiretap laws. On class certification, the *Gmail* court concluded that individual issues of whether putative members impliedly consented to Google's alleged interceptions would predominate over common issues, explaining:

there is a panoply of sources from which email users could have learned of Google's interceptions [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.

2014 WL 1102660, at *17-18. The trial court here was well within its discretion to apply this well-reasoned analysis to this case. (JA 0955-60.)

As in *Gmail*, the evidence before the trial court showed that putative class members could become aware of the automated processing in Gmail from a myriad of sources. For example, Google's public Help page explains that "automatic scanning and filtering technology is at the heart of Gmail" and "Gmail scans

defendants recorded their communications without consent because liability determinations "would require intense individual examinations").

. . . all messages" for various purposes including "show[ing] relevant ads" (JA 0681.) To resolve the issue of implied consent, a fact-finder would need to determine whether each putative class member was aware of this explanation of automated scanning. (JA 0960; 0962.) And this is just one of numerous disclosures that would need to be considered for each claimant.

Further, Google showed that dozens of *non*-Google sources would be relevant in evaluating the knowledge of any individual member of the putative class. The knowledge exception could apply to anyone who has seen one of the thousands of articles over the last 11 years discussing the automated scanning features of Gmail, among many other potential sources of knowledge.²⁶ (JA 0041 ¶¶ 6-7; 0171-203; 0218-459.)

Given the inherently individualized evidence needed to resolve issues of knowledge, the trial court was well within its discretion in denying class certification. Certainly, Plaintiff cannot show that "the decision falls outside the range of reasonable

²⁶ Further complicating the analysis, a fact-finder would also need to determine *when* each individual first became aware of scanning to resolve the applicable statute of limitations. "In Massachusetts, a statute of limitations begins to run when the plaintiff learned or should reasonably have learned that he has been harmed." *Moelis v. Berkshire Life Ins. Co.*, 451 Mass. 483, 491 (2008).

alternatives," as she must. *L.L. v. Com.*, 470 Mass. 169, 185 n.27 (2014).

C. Plaintiff's Response To The Individualized Issues Of Knowledge Is Meritless.

While Plaintiff concedes that certain members of her proposed class would be "aware that Google scans some emails," she claims this is insufficient to support implied consent because "Google only scans certain emails." (POB 42.) This tortured argument distorts the applicable law and should be rejected.

Indeed, the *Jackson* case that Plaintiff cites for her argument actually undermines her position. In *Jackson*, the defendant appealed the denial of a motion to suppress two phone calls allegedly recorded in violation of the Act.²⁷ *Jackson*, 370 Mass. at 503. In these calls, the defendant had stated that he knew he was being recorded. *Id.* at 504. He argued this did not constitute "actual knowledge" because the statements were "nothing more than mere speculation . . . because the [person who recorded the calls] never acknowledg[ed] that he was taping the calls."

²⁷ Plaintiff makes much of the fact that the trial court in *Jackson* suppressed three communications as violating the Act where the defendant had not indicated he knew he was being recorded. (POB 41-42 n.6.) But the SJC did not have the opportunity to assess whether those calls were properly suppressed under the correct "actual knowledge" standard because they were "not before [the court] on appeal." *Jackson*, 370 Mass. at 504-05. Accordingly, they say nothing about the SJC's holding in *Jackson*.

Jackson, 370 Mass. at 505-06. The SJC rejected this argument, explaining:

actual knowledge is proved where there are clear and unequivocal objective manifestations of knowledge, for such indicia are sufficiently probative of a person's state of mind as to allow an inference of knowledge and to make unnecessary any further requirement that the person recording the conversation confirm the caller's apparent awareness by acknowledging the fact of the intercepting device.

Id. at 507 (emphasis added). *Jackson* thus confirms that the appropriate focus is on the claimant's "state of mind" and not on "the fact of the intercept[ion]." *Id.* That is, if a claimant subjectively believes that a communication can be intercepted and "continue[s] to speak in apparent indifference to the consequences," that "state of mind" amounts to implied consent that the claimant's communications can be intercepted. This is so regardless of whether any particular communication is *in fact* intercepted. *Id.* Take, for example, the situation where a store displays a sign indicating that it is monitored by surveillance cameras. By choosing to shop in that store, the customer consents to being videotaped. Her consent is not affected by the fact that, for some reason, the surveillance camera was not working at the time she was in the store. Indeed, the SJC has found consent in a nearly analogous situation. *Com. v. Rivera*, 445

Mass. 119, 134 (2005) (reaffirming *Jackson* and holding that defendant could be presumed to have knowledge of an audio recording device that was part of a video camera in plain view, without regard to whether the device in fact recorded all communications); see also *Glik v. Cunniffe*, 655 F.3d 78, 86-87 (1st Cir. 2011) (referring to *Jackson* and explaining that "the secrecy inquiry turns on notice, i.e., whether, based on objective indicators, such as the presence of a recording device in plain view, one can infer that the subject was aware that she *might* be recorded.") (emphasis added).

These authorities conclusively rebut Plaintiff's effort to avoid the implied consent issues here. As in *Jackson*, if an individual knows that an email sent to a Gmail user can be subject to automated scanning and continues to send emails "in apparent indifference to the consequences," that is sufficient for implied consent, regardless of whether some emails may bypass the scanning process. *Jackson*, 370 Mass. at 507.²⁸

²⁸ Even if Plaintiff were correct that a user must have actual knowledge that a particular email had been intercepted, the inquiry into whether each user knew each email was scanned would be similarly individualized. The Court could not merely presume, as Plaintiff suggests, that "no Class member could have actual knowledge of whether Google was scanning their emails." (POB 41.) Google would be entitled to present defenses against those users who did have actual knowledge. See *Wal-Mart Stores, Inc. v. Dukes*,

D. Alternative Bases For Affirming The Trial Court's Denial Of Class Certification.

1. Plaintiff Cannot Identify The Instances Of Scanning On A Classwide Basis.

The trial court could have also denied certification based on the individual issues involved in identifying precisely which emails were scanned. To justify classwide treatment, Plaintiff was required to demonstrate a viable method to identify the specific emails that were scanned by the alleged wrongful processes at issue, among the millions (if not billions) of emails implicated by the proposed class. At class certification, Plaintiff claimed this immensely complex task was amenable to classwide treatment because "all" emails in certain broad categories are subject to uniform scanning. (See, e.g., JA 0474-75.) But these assertions are demonstrably false. Plaintiff claims that "all" emails sent to Gmail users after August 2010 are scanned for "commercial purposes." But, during that time, Gmail's scanning processes were subject to numerous exceptions as set forth in the record before the trial court. For example, for a time, emails that Gmail determined to be potential spam were not scanned for the purpose of targeted advertising. (JA 0822-24 ¶¶ 25-27.) Similarly, in certain instances where a Gmail user opened or sent an email from a mobile

131 S. Ct. 2541, 2561 (2011).

device (which accounts for a significant amount of all activity on Gmail), Gmail's scanning processes would not scan those emails for the purpose of providing targeted advertising. (JA 0814-19 ¶¶ 11-17.) Plaintiff proposed no workable method to address these, or any other, exceptions to Gmail's scanning.²⁹

Plaintiff's reliance on Smart Labels as a proxy for illegal scanning is misplaced. There are numerous instances in which an email that had not been scanned for targeted advertising would include a Smart Label, as reflected in the undisputed evidence in the case. (JA 0824-25 ¶¶ 28-32.)

2. The Proposed Class Is Unascertainable.

If "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) (quotation and citation omitted). For this reason, a plaintiff must generally identify some existing source of records, data, or other centralized evidence that

²⁹ Plaintiff may attempt to argue in reply that her expert, Michael Helmstadter, determined that Google uniformly scans emails. The Court should disregard Mr. Helmstadter's purported "expert" opinions as incorrect and unreliable for all of the reasons set forth in Google's motion to strike Mr. Helmstadter's analysis. See Memo. ISO Google's Mot. to Strike Pl.'s Expert Helmstadter's Analysis ("Mot. to Strike"); Reply ISO Mot. to Strike.

can be used to identify the members of the proposed class. See *Waters v. EarthLink, Inc.*, No. 01-cv-0628, 2006 WL 1549685, at *7 (Mass. Super. Ct. May 10, 2006) (denying certification where plaintiff failed to "present any evidence" that individuals affected by defendant's conduct "could be gleaned from some set of business records or data") (citation omitted).

Here, [REDACTED]
[REDACTED]
[REDACTED]
(JA 0829-30 ¶¶ 51-52.) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] (JA 0823-24 ¶ 27; 0828 ¶ 45.) Even then, it may be impossible to determine if the proposed class member's email were scanned. (JA 0815-19 ¶¶ 14-17; 0822-24 ¶¶ 25-27; 0825 ¶ 31; 0829 ¶ 51.)³⁰

³⁰ At class certification, Plaintiff proposed to ascertain the class by having individuals submit claims to identify themselves as class members. (JA 0474.) Plaintiff's proposal would not be "administratively feasible" because it would require the parties to review potentially millions of claims and resolve an untold number of disputes over whether individual claimants meet the specific requirements of class membership, like whether a claimant meets the specific criteria for Massachusetts residency (which Plaintiff did not identify). See, e.g., *Carrera v. Bayer Corp.*, 727 F.3d 300, 308-09 (3rd Cir. 2013) (rejecting plaintiffs' contention that "the class is ascertainable using affidavits of class members" to

Even if the proposed class members could be identified, the result would be a massively overbroad collection of people, many of whom have no claim. For example, Plaintiff's proposed class would indiscriminately encompass people who sent emails to Gmail users with knowledge of Google's scanning practices (Section IV.B., supra); people with both a Gmail and non-Gmail account who are bound to Google's terms (JA 0545 ¶ 7); and people whose emails were never scanned (Section IV.D.1., supra). A class cannot be certified under these circumstances. *Kwaak*, 71 Mass. App. Ct. at 300-02 (denying certification where court could not "conclude that the class . . . consists of [class members] similarly situated and similarly injured."); *Waters*, 2006 WL 1549685, at *7 (denying certification where "some may not have experienced any delays in the receipt or delivery of their e-mail messages"); *In re Neurontin Mktg. and Sales Practices Litig.*, 244 F.R.D. 89, 113 (D. Mass. 2007) (denying certification where plaintiffs were unable to identify "a single case where a court certified an overbroad class with members who were not injured under such a theory."). The trial court did not abuse its discretion in declining to certify this massively overbroad class.

E. The Court Properly Refused To Certify A Sub-Class Of Google Apps Users.

identify purchasers of the disputed product).

This Court has no basis to assess Plaintiff's argument that the trial court should have certified a sub-class of Google Apps users because there is no evidence relevant to this sub-class in the record. *Com. v. Marchionda*, 385 Mass. 238, 242 (1982) ("An issue not fairly raised before the trial judge will not be considered for the first time on appeal.") (citations omitted). The trial court did not abuse its discretion in denying certification of a sub-class that Plaintiff never suggested until six days after the hearing on her motion for class certification. Plaintiff represents to this Court that she "set forth the appropriateness of [a Google Apps] subclass" in her briefing. (POB 46-48.) This is demonstrably false. The out-of-context statements regarding Google Apps to which Plaintiff points had nothing to do with a sub-class of Google Apps users. To the contrary, Plaintiff merely identified for the trial court that the "Gmail users" identified in her class definition could include both Gmail and Google Apps users.³¹

At most, Plaintiff argued (for the first time in her reply) that class members who exchanged emails with Google Apps users would not be subject to the

³¹ Google respectfully requests that the Court review Plaintiff's briefs in support of her Motion for Class Certification, (JA 0466-88; 0922-34), which show the context of Plaintiff's statements and make clear she never raised the issue of a sub-class.

same individualized consent problems as class members. But, in making this belated argument, she did not assert or even mention a potential sub-class. Even if she had raised such a sub-class in her reply, this would have been inappropriate, and the trial court could have refused to consider it.³² See *Rubenstein v. Liberty Mut. Ins. Co.*, No. 90-cv-1687, 1991 WL 787069, at *9 (Mass. Super. Ct. Oct. 3, 1991). As the trial court acknowledged, the parties had no opportunity to brief critical issues related to a potential Google Apps sub-class. (JA 0962-64.) For example, Plaintiff has never shown that she actually emailed with a Google Apps user, thus it is unclear whether she would be a member of her proposed sub-class. (JA 0963-64.)

Further, in denying Plaintiff's untimely request to certify a Google Apps sub-class, the trial court invited Plaintiff to bring another class certification motion to address such a sub-class, yet Plaintiff declined. (JA 0963.) She should not now be rewarded for her failure to diligently pursue her claims.

V. THE TRIAL COURT ERRED IN DENYING GOOGLE'S MOTION TO DISMISS.

A. Google's Conduct Is Excepted From Liability Under The OCB Exception To The Act.

For the reasons discussed above in Section

³² Plaintiff faults Google for "never den[ying] the validity of this sub-class," (POB 48-49), but Google never had the opportunity to address this issue.

III.B.1, the trial court further erred in holding that Google's conduct did not fall into the OCB exception as a matter of law. (JA 0020-21.) While Google's evidence on summary judgment confirmed the legitimate business purposes of its automated scanning, these issues were already apparent on the face of the Complaint (JA 0006-07 ¶¶ 2, 7-9), and should have been resolved in Google's favor on its Motion to Dismiss. Plaintiff's Complaint recognizes that Gmail is "a 'free' service" that is made possible by "selling advertising" on Gmail, (JA 0007 ¶ 8) and, moreover, concedes that Google applies automated systems to scan emails, not to engage in surreptitious surveillance, but to "acquire[] keywords" for the purpose of "send[ing] ads related to those keywords" (JA 0007 ¶ 9.) These are legitimate business purposes exempting Google from liability as a matter of law.

CONCLUSION

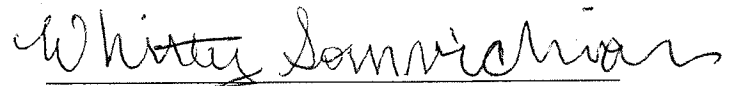
Google respectfully asks this Court to affirm the trial court's decisions on the motions for summary judgment and class certification and reverse the trial court's determination on the motion to dismiss.

Dated: December 18, 2015

Respectfully submitted,

Google Inc.

By its Attorneys,

 (JD)

Michael G. Rhodes (*pro hac vice*)
Whitty Somvichian (*pro hac vice*)
Kyle C. Wong (*pro hac vice*)
Karen L. Burhans (BBO 679017)
COOLEY LLP
101 California Street, 5th Flr.
San Francisco, CA 94111-5800
Tel.: (415) 493-2000
Fax: (415) 493-2222
rhodesmg@cooley.com
wsmovichian@cooley.com
kwong@cooley.com
kburhans@cooley.com

- and -

Robert B. Lovett (BBO 561691)
Michael N. Sheetz (BBO 548776)
Cooley LLP
500 Boylston St.
Boston, MA 02116-3736
Tel.: (617) 937-2300
Fax: (617) 937-2400
rlovett@cooley.com
msheetz@cooley.com

Counsel for Defendant-
Appellee/Cross-Appellant

ADDENDUM

KeyCite Yellow Flag - Negative Treatment
Unconstitutional or Preempted **Validity Called into Doubt by** Jean v. Massachusetts State Police, 1st Cir.(Mass.), June 22, 2007

KeyCite Yellow Flag - Negative Treatment Proposed Legislation

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.

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

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.

Notes of Decisions (304)

M.G.L.A. 272 § 99, MA ST 272 § 99

Current through Chapter 144 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]
[REDACTED] [REDACTED]
[REDACTED] The results are then forwarded to a [REDACTED] 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] [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]
[REDACTED]
[REDACTED]
[REDACTED] see text below). Other issues may [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], there is content that COB [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

sent to the user, a [REDACTED] and so on.

[REDACTED] 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 the [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] is run on servers physically located in [REDACTED]. The code that implements the COB process is run on servers physically located in [REDACTED]. The code that implements the User Model process is run on servers physically located in [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 the [REDACTED] and the User Model process; (2) that the [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] [REDACTED] [REDACTED] 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] [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] [REDACTED] [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] A [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 [REDACTED] [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 [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. The emails sent to Gmail users in Categories 2 and 3 [REDACTED] [REDACTED] to the Gmail system. For instance, [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] The non-Gmail account user [REDACTED] Thus, the non-Gmail account user [REDACTED]

[REDACTED] A message identified [REDACTED]
[REDACTED] for purposes of
delivering targeted advertising. Google's systems [REDACTED]
[REDACTED] in this process. [REDACTED] email messages sent to
Gmail users [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]
[REDACTED] Google's [REDACTED] 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]

[REDACTED]

According to Kapadia, Google does [REDACTED] which emails were [REDACTED] apart from the emails themselves. Kapadia is [REDACTED] [REDACTED] each individual email recipient. In an instance where a non-Gmail user sends an email to a Gmail user, Kapadia is [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]

██████████ is also subject to various exceptions. The emails in Category 2 refer to emails subjected to ██████████ which was implemented ██████████ ██████████ advertising. ██████████ scans emails ██████████ ██████████ is an automated process that does not involve human review. For example, ██████████ 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. ██████████ 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. ██████████ in some circumstances to assign a "Smart Label" to an email in a section 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 ██████████.

Gmail users have the option of opting out of personalized advertising on Google's website and information identified ██████████ 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 ██████████ This collective information is used to select and display ads to the Gmail user.

██████████ is not applied to all emails sent to Gmail users. ██████████ ██████████ an email received by a Gmail email account generally ██████████ ██████████ Although many ██████████

approximately [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] that would, in
turn, impact whether a particular email is actually scanned. [REDACTED]
Google does [REDACTED]
[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
[REDACTED] 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]
[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]
[REDACTED] rather, it [REDACTED]
[REDACTED] come from emails. Google does [REDACTED] about which emails were processed by

the User [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] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] For instance, Google [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED] [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, is 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.

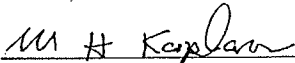
The court, however, does not foreclose the plaintiff from pursuing such a class, although certain substantial impediments to certification do suggest themselves. First, the record presently before the court appears to establish that many Google Apps customers do not permit Google to place advertising 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

Marquis

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION
NO. 11-2808-BLS1

ADJUDGE SET
01.17.12
C.G.K.
K.L.B.
R.C.L.
K.K.+Z.
J.P.R.
J.P.Z.
J.A.
C.ILLP
M.G.R.
W.S.

DEBRA L. MARQUIS

v.

GOOGLE INC.

MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT GOOGLE INC.'S MOTION TO DISMISS

(LAT)

This action arises from the alleged monitoring of emails by defendant Google Inc. ("Google") in order to sell advertisements based on keywords that appear in those emails. Google operates Gmail, which is an electronic communications or email service. The plaintiff, Debra L. Marquis, represents a putative class of Massachusetts residents who have non-Gmail email accounts, but who exchange emails with Gmail users. Marquis alleges that Google's monitoring of emails sent from non-Gmail email accounts violates the Massachusetts wiretap statute, G.L. c. 272, § 99.

Google has now moved to dismiss this action on the grounds that the wiretap statute does not apply to email communications or to its conduct. For the reasons discussed below, Google's motion to dismiss is denied.

BACKGROUND

The court takes as true all well-pled factual allegation set forth in Marquis's Complaint, see *Marshall v. Stratus Pharms., Inc.*, 51 Mass. App. Ct. 667, 670-71 (2001). Marquis is a Massachusetts resident who has a non-Gmail email account.

Compl. ¶ 3. Google is a Delaware corporation with its principal place of business in California. Compl. ¶ 4. It operates Gmail, which is an electronic communication service that is free to its users. Compl. ¶¶ 6-8. While Google does not charge Gmail account holders for using its service, Google generates revenue through advertisements that it presents to Gmail users. Compl. ¶ 8. Google intercepts and scans emails sent from non-Gmail users, such as Marquis, in order to find keywords or content in the emails that will enable it to target advertisements specifically at Gmail users. Compl. ¶ 9. Once targeting individual emails, Google now focuses on numerous emails to find keywords. Compl. ¶ 11. This system is known as “interest-based advertising.” Compl. ¶ 11.

Marquis has an America-On-Line (“AOL”) email account that she has used since the late 1990s. Compl. ¶ 13. While she routinely exchanged emails with Gmail users, Marquis did not consent to Google’s secret interception, disclosure, or scanning of her emails. Compl. ¶¶ 12, 14. Marquis seeks to represent a class of Massachusetts residents who have non-Gmail email accounts and who exchange emails with Gmail users, and who have their emails intercepted and/or scanned without their consent. Compl. ¶ 15.

Marquis alleges that Google’s conduct violates the Massachusetts Wiretap statute, G.L. c. 272, § 99. The statute “was enacted to give due protection to the privacy of individuals by barring the secret use of electronic surveillance devices for

eavesdropping purpose” *Dillon v. Massachusetts Bay Transp. Auth.*, 49 Mass. App. Ct. 309, 310 (2000). It prohibits any person from intercepting or attempting to intercept “any wire or oral communication.” G. L. c. 272, § 99(C)(1). A wire communication is defined as “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.” *Id.* at § 99(B)(1). An intercepting device does not include “any telephone or telegraph instrument, equipment facility, or a component thereof . . . being used by a communications common carrier in the ordinary course of business.” *Id.* at § 99(B)(3).

Google has now moved to dismiss the Complaint. First, it contends that the Massachusetts wiretap statute does not apply to electronic communications, and if it does, then it is preempted by the federal wiretap statute. Second, it argues that Marquis was aware that Google intercepted and scanned her emails, and the statute requires that the interception be done secretly. Third, Google’s alleged interception occurred in the ordinary course of business and is therefore exempted from the statute.

DISCUSSION

In order to withstand a motion to dismiss, a plaintiff’s complaint must contain “allegations plausibly suggesting (not merely consistent with) an entitlement to relief,

in order to reflect [a] threshold requirement . . . that the plain statement possess enough heft to sho[w] that the pleader is entitled to relief.” *Iannacchino v. Ford Motor Co.*, 451 Mass. 623, 636 (2008), quoting *Bell Atl. Corp. v. Twombly*, 127 S. Ct. 1955, 1966 (2007) (internal quotations omitted). While a complaint need not set forth detailed factual allegations, the plaintiff is required to present more than labels and conclusions, and must raise a right to relief “above the speculative level . . . [based] on the assumption that all the allegations in the complaint are true (even if doubtful in fact).” *Id.* See also *Harvard Crimson, Inc. v. President & Fellows of Harvard Coll.*, 445 Mass. 745, 749 (2006). The court will examine the Complaint under this standard.

Google’s first argument is that the Massachusetts wiretap statute does not include a prohibition against monitoring emails. In essence, it contends that had the Legislature desired to include such electronic communications in the statute, then it would have done so expressly.¹ The Massachusetts wiretap statute was originally intended to mirror its federal counterpart. See *O’Sullivan v. NYNEX Corp.*, 426 Mass. 261, 264 (n.5) (1997). In 1986, the federal statute was “recognized to be hopelessly out of date,” and it was amended by the Electronic Communications Privacy Act (“ECPA”) in order to cover “electronic communication,” which encompasses email. *Dillon*, 49 Mass. App. Ct. at 314-15 (citations omitted); 18

¹ Google presents G.L. c. 276, § 1B, which expressly defines “electronic communication services” and “remote computing services,” as one such example. In contrast, the Massachusetts wiretap statute does not define these terms.

U.S.C. § 2510(12). The Massachusetts Legislature did not provide for a similar amendment. However, “the fact that there has been no amendment of the Massachusetts statute comparable to the Congressional action of 1986 does not bar us from reading [an exception] so as to preserve it in its intrinsic intended scope and maintain its viability in the broad run of cases.” *Dillon*, 49 Mass. App. Ct. at 315.

This court declines to accept Google’s contention that the Massachusetts wiretap statute does not prohibit the secret interception of emails. First, the statute’s definition of “wire communications” is sufficiently broad to include electronic communications, as it includes “the aid of wire, cable, or *other like connection* between the point of origin and the point of reception.” G.L. c. 272, § 99(B)(1) (emphasis supplied). Permitting the interception of private emails, while prohibiting the same conduct for oral telephone conversations, is an inconsistency that contravenes the purpose of the statute. Second, a Massachusetts court has recently held that the Massachusetts wiretap statute cover email, and the court finds its reasoning persuasive. See *Rich v. Rich*, 2011 WL 3672059, *5 (Mass. Super. July 8, 2011) (McGuire, J.).

At this stage of the litigation, the court must accept the factual allegations of the Complaint. Marquis alleges that Google intercepts and scans private emails that she sends from her AOL account to Gmail account users, and that she did not consent to Google’s interception. Compl. ¶¶ 9, 13-14. This alleged conduct violates

the Massachusetts wiretap statute.

Google's second argument is that federal law preempts the Massachusetts wiretap statute. Federal law may preempt state law "when it explicitly or by implication defines such an intent, or when a State statute actually conflicts with Federal law or stands as an obstacle to the accomplishment of Federal objectives. Whether a Federal statute preempts State law is ultimately a question of Congress's intent." *City of Boston v. Commonwealth Employment Relations Bd.*, 453 Mass. 389, 396 (2009) (internal citations omitted). A court should be hesitant to find preemption, as "[u]nless Congress's intent to do so is clearly manifested, a court does not presume that Congress intended to displace State law on a particular subject. . . ." *Id.*

Prior to the 1986 amendments to the federal wiretap statute, the Supreme Judicial Court determined that the federal statute did not preempt the Massachusetts wiretap statute. See *Commonwealth v. Vitello*, 367 Mass. 224, 249-53 (1975). Google maintains that the ECPA's comprehensive regulatory scheme indicates Congress's intent to occupy the field. However, this is insufficient to warrant a finding that the federal wiretap statute preempts the Massachusetts wiretap statute. The ECPA does not contain language expressly, or by implication, preempting state law. See 18 U.S.C. §§ 2510-2522. In addition, the ECPA does not occupy the entire field of interception of electronic surveillance, as Google contends. As long as the Massachusetts wiretap statute does not conflict with the federal wiretap statute, then

it is a valid law under principles of federalism. *Vitello*, 367 Mass at 247 (“[A] State statute may adopt standards more stringent than the requirements of Federal law.”). As Google itself notes, the federal wiretap statute prohibits the secret interception of electronic communications, just like the Massachusetts wiretap statute, see *supra*. In the absence of manifest Congressional intent to preempt state law, the ECPA does not preempt the Massachusetts wiretap statute.

Google’s next contention is that while the Massachusetts wiretap statute prohibits “secret” interceptions, its advertisement policy is publicly disclosed and transparent. As a result, Google argues that its conduct does not violate the Massachusetts wiretap statute. Under the statute, an interception “means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication. . . .” G.L. c. 272, § 99(B)(4). Marquis alleges that Google “secretly” intercepts her electronic communications with Gmail users. Compl. ¶¶ 14, 27. To rebut that allegation, Google has submitted an affidavit that includes Google’s Terms of Service and Privacy Center screen. See Burhans Affidavit at Tabs 1 and 2. These documents illustrate that Google’s “interest-based advertising” is fully disclosed.

The Burhans Affidavit does not rebut the Complaint’s allegations. First, Google’s attempt to introduce documents outside the pleadings is improper at the

motion to dismiss stage.² Second, the court accepts as true Marquis's allegation that Google secretly intercepted her electronic communications with Gmail users. Additionally, Marquis is entitled to the reasonable inference that she, as an AOL account holder, would not be privy to or have notice of Google's Terms of Use and Privacy Center policy for Gmail users. The Complaint alleges sufficient facts that Google secretly intercepted electronic communications between non-Gmail users and Gmail users.

Google's final argument is that it is exempt from liability because it is a communications common carrier, and that it conducted the alleged interceptions "in the ordinary course of its business." G.L. c. 272, § 99(B)(3). In support of this contention, Google presents two cases that involve employers who secretly intercepted communications between their employees and third-parties. Google's reliance on these cases is misplaced, as it does not have an employer-employee relationship with Gmail users. While Gmail is a free service, Google generates revenue through selling advertising. Compl. ¶ 8. It intercepts and scans emails sent to Gmail users by non-Gmail users such as Marquis in order to find keywords so that

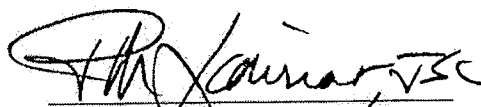
² "In evaluating a rule 12(b)(6) motion, we take into consideration the allegations in the complaint, although matters of public record, orders, items appearing in the record of the case, and exhibits attached to the complaint, also may be taken into account." *Schaer v. Brandeis Univ.*, 432 Mass. 474, 477 (2000) (quotation omitted). Google's Terms of Use and Privacy Center policy, external to the Complaint, are not appropriate for consideration at this stage.

it can target Gmail users with relevant advertisements. Compl. ¶¶ 9, 11. At this preliminary stage, the court cannot conclude as a matter of law that intercepting and scanning emails for purposes of “interest-based advertising” is “in the ordinary course of [Google’s] business” under the Massachusetts wiretap statute.

ORDER

For the foregoing reasons, Defendant Google Inc.’s Motion to Dismiss is

DENIED.



Peter M. Lauriat
Justice of the Superior Court

Dated: January 17, 2012

**CERTIFICATE OF COMPLIANCE
PURSUANT TO RULE 16(K) OF THE
MASSACHUSETTS RULES OF APPELLATE PROCEDURE**

I, Karen L. Burhans, hereby certify that the foregoing brief complies with the rules of 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);

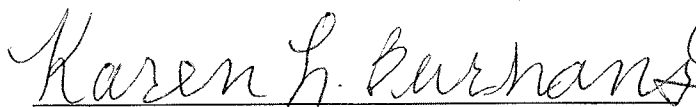
Mass. R.A.P. 16(e) (references to the record);

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

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

Mass. R.A.P. 18 (appendix to the briefs); and

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



KAREN L. BURHANS (BBO 679017)
kburhans@cooley.com
COOLEY LLP
101 California Street
5th Floor
San Francisco, CA 94111
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

CERTIFICATE OF SERVICE

I, Karen L. Burhans, attorney for Defendant-Appellee/Cross-Appellant Google Inc., hereby certify under the penalties of perjury that, on this 18th day of December, 2015, I caused to be served by hand delivery to counsel for the Plaintiff-Appellant/Cross-Appellee Debra L. Marquis, two copies of the foregoing document:

John Peter Zavez, Esq.
Jason B. Adkins, Esq.
Jeffrey Thorn, Esq.
ADKINS, KELSTON & ZAVEZ, P.C.
90 Canal St., Suite 500
Boston, MA 02114
Tel.: (617) 367-1040
Fax: (617) 742-8280
jzavez@akzlaw.com
jadkins@akzlaw.com
jthorn@akzlaw.com

 (38)
KAREN L. BURHANS (BBO 679017)