

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]
[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]
[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]

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

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

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

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 account holder. 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] Gmail users are not required to identify their state of residency in order to create a Gmail account.

Declaration of Brandon Long and Google Apps

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

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

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

DISCUSSION

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

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

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

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

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

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

Predominance

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Google Apps and Ascertainability

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

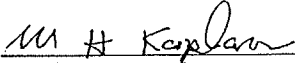
The court, however, does not foreclose the plaintiff from pursuing such a class, although certain substantial impediments to certification do suggest themselves. First, the record presently before the court appears to establish that many Google Apps customers do not permit Google to place advertising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

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

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

ORDER

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



Mitchell H. Kaplan
Justice of the Superior Court

Dated: June 19, 2014