United States District Court
For the Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: GOOGLE INC. GMAIL LITIGATION THIS DOCUMENT RELATES TO: **ALL ACTIONS**	Case No.: 13-MD-02430-LHK ORDER DENYING PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

In this consolidated multi-district litigation, Plaintiffs Keith Dunbar, Brad Scott, Todd Harrington, Ronald Kovler, Matthew Knowles, A.K. (next friend to Minor J.K.), Brent Matthew Scott, Robert Fread, and Rafael Carrillo, individually and on behalf of those similarly situated (collectively, "Plaintiffs"), allege that Defendant Google, Inc., has violated state and federal anti-wiretapping laws in its operation of Gmail, an email service. *See* ECF No. 98-4 ("FACC"). Pending before the Court is Plaintiffs' Motion for Class Certification, in which Plaintiffs move to certify four Classes and three Subclasses. *See* ECF No. 87-26 ("Mot."). Google has filed an Opposition, *see* ECF No. 101-2 ("Opp."), and Plaintiffs have filed a Reply, *see* ECF No. 112-2 ("Reply"). The Court held a hearing on the Motion on February 27, 2014. *See* ECF No. 148 ("Tr."). Having considered the briefing, the record in this case, and the oral arguments presented at the hearing, the Court DENIES Plaintiffs' Motion for Class Certification.

United States District Court
For the Northern District of California

I. BACKGROUND

A. Factual Background

Plaintiffs challenge Google's operation of Gmail under state and federal anti-wiretapping laws. In the FACC, Plaintiffs seek damages, injunctive relief, and declaratory relief on behalf of a number of classes of individuals who either use Gmail or exchange messages with those who use Gmail for Google's interception of emails over a period of several years. FACC ¶¶ 254-349. Specifically, Plaintiffs state causes of action 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). FACC ¶¶ 8-14.

1. Email Users Implicated

Google's operation of Gmail implicates several different groups of email users, whose interactions with Google's processes are slightly different. Accordingly, the Court begins by providing background on the types of email users implicated in this litigation and explaining the agreements with Google that each of these types of users encounter as they set up their email accounts.

First, Google provides a free web-based email service called Gmail. ECF No. 103-1, ("Chin Decl.") ¶ 2. Users of this service can sign up for an "@gmail.com" account on a Google webpage, titled "Create an Account." *Id.* ¶ 10. In the process of creating an account, users of Google's free Gmail service (to whom the Court will refer as "Gmail users") must check a box indicating that they agree to be bound by Google's Terms of Service ("TOS") and Privacy Policy. *Id.* ¶ 9. The "Create an Account" page links to webpages containing the relevant TOS and Privacy Policy. *See id.*, Ex. F. Named Plaintiff J.K. went through this process to create the Gmail account at issue in the instant litigation. *Id.* ¶ 10.

Second, Google offers a service known as "Google Apps" to customers including businesses, educational organizations, and internet service providers ("ISPs"). *Id.* ¶ 3. Through Google Apps, these customers can provide Google services, including Gmail, Google Calendar, and Google Docs, to their employees, students, or customers (to whom the Court refers as "end users"). *Id.* The end users do not receive "@gmail.com" email addresses. *Id.* Rather, their email addresses contain the domain name of the entity that contracts with Google to provide the services. *Id.* The business or educational institution that contracts with Google for Google Apps (to whom the Court refers as "Google Apps Administrators") is responsible for overseeing the creation of the accounts of end users. *Id.*

The instant litigation concerns two sets of Google Apps end users. The first set is comprised of end users of Cable One, an ISP that contracts with Google to provide Google Apps-related services to its customers. FACC ¶ 99. Cable One contracted with Google and agreed to ensure that its end users agreed to the Google Apps TOS, which are, in all respects relevant to the instant litigation, identical to the Gmail TOS. *Id.* Importantly, Google's agreement with Cable One precludes Google from displaying advertisements in connection with the Google Apps services. ECF No. 86-16 ("Rommel Decl."), Ex. Q ¶ 1.7. Named Plaintiff Keith Dunbar is a Cable One customer who seeks to represent a class of Cable One end users. FACC ¶ 8.

The second set of Google Apps end users in this litigation are Google Apps for Education users. Like Cable One, educational institutions that provide Google Apps services agreed, in their contracts with Google, to obtain the necessary authorization from end users to enable Google to provide the services. Chin Decl. ¶¶ 3-4. The contracts further required Google to comply with Google's Privacy Policies. *Id.* ¶¶ 7-8. Moreover, like Cable One end users, Google Apps for Education end users also did not receive advertisements. FACC ¶ 244. Named Plaintiff Rafael Carrillo, who was a student of the University of the Pacific, and named Plaintiff Robert Fread, a student at the University of Hawaii, were end users of Google Apps for Education as a result of

United States District Court
For the Northern District of California

those institutions' use of Google Apps. *Id.* ¶¶ 223-44. Fread and Carrillo now seek to represent a class of Google Apps for Education end users. *Id.* ¶ 13.

Third, Plaintiffs include individuals who do not use any of Google's services, but are nevertheless impacted by the interceptions because these individuals send emails to or receive emails from Gmail users. *Id.* ¶¶ 251-53. The Court will refer to these individuals, whom named Plaintiffs Brad Scott, Todd Harrington, Ronald Kovler, Matthew Knowles, and Brent Scott seek to represent, as "non-Gmail users." *Id.*

2. The Operation of Gmail and Accused Devices

Google's processing of Gmail has changed twice during the class periods: in [redacted] 2010 and [redacted] 20[redacted]. FACC ¶¶ 39, 79. While Plaintiffs have accused various steps of the Gmail processing of unlawful interceptions in their pleadings, they clarify the scope of their contentions in their Reply in support of the instant Motion. Reply at 6. Specifically, Plaintiffs clarify that Google's processing of emails with respect to only two sets of email transmission is at issue. *Id.* First, Plaintiffs are concerned with the processing of emails sent *to* Gmail users by putative Class members who are Gmail users, Google Apps users, or non-Gmail users. *Id.* Second, Plaintiffs are concerned with the processing of email messages received *by* putative Class members who are Google Apps and Gmail users. *Id.* Plaintiffs clarify that these two sets of challenged interceptions occur as a result of three devices that process Google's emails: (1) Content Onebox ("COB"), (2) Medley Server, and (3) Changeling. *Id.* n.18. Accordingly, Plaintiffs clarify that they are not seeking to certify classes to accuse the CAT2 Mixer, which had previously been accused, of unlawful interceptions.[1] *Id.*

With respect to Google's processes before [redacted] 2010, Plaintiffs contend that Google used the CAT2 Mixer, Medley Server, and ICEbox Server to read the content of emails received by

[1] The CAT2 Mixer processes emails sent from an @gmail.com account, which Plaintiffs have not challenged here, and also had a role in the processing of messages received by @gmail.com accounts before [redacted] 2010, as discussed in this section.

@gmail.com email addresses for keywords. FACC ¶¶ 25-30. Plaintiffs contend that Google extracted concepts from the content of the emails. FACC ¶¶ 25-28; Mot. at 4. Moreover, Plaintiffs contend that Google acquired metadata from the content of the email messages, and that this metadata was stored in secret user profiles. FACC ¶¶ 73-78; Mot at 4, 6. [redacted]

Between [redacted] 2010 and [redacted] 20[redacted], Plaintiffs contend that Google routed all emails received by Gmail users [redacted] through the COB. FACC ¶ 39; Mot. at 4. Through the COB, Plaintiffs contend, Google acquired message content and meaning even when the user was not receiving a personalized advertisement. *Id.* The information that the COB extracted was used to create metadata and annotations, which are allegedly stored in secret user profiles. FACC ¶¶ 73-78; Mot. at 5.

Finally, with respect to post-[redacted] 20[redacted] processing, Plaintiffs contend that Google moved the COB [redacted]. FACC ¶ 79; Mot. at 5-6. [redacted].[2] FACC ¶ 89; Mot. at 5-6.

3. Google's Disclosures

Google points to a number of documents publically available through its various webpages that discuss the challenged interceptions at issue in the instant litigation to contend that its users were aware of the interceptions. While it is clear that Gmail users had to indicate that they read some of these disclosures as part of the account registration process, it is not clear from the record

[2] In their Motion for Class Certification, Plaintiffs also suggest that transcribed phone calls through Google Voice are subject to COB processing. Mot. at 6. However, this theory appears nowhere in the FACC, and the Court therefore does not consider it here.

to which disclosures the two groups of Google Apps users were exposed in their account-registration process. Accordingly, the Court discusses disclosures to the two sets of Google Apps users separately below.

First, Google points to the TOS to which all Gmail users had to agree to create a Gmail account. Gmail users were alerted to the TOS when they created a Gmail account. Chin Decl. ¶ 9. The first TOS was in effect from April 16, 2007, to March 1, 2012; the second was in effect from March 1, 2012 to November 11, 2013; and a third has been in effect since November 11, 2013. *Id.* ¶¶ 14-15. The 2007 TOS stated that:

> Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service. For some Services, Google may provide tools to filter out explicit sexual content. These tools include the SafeSearch preference settings . . . . In addition, there are commercially available services and software to limit access to material that you may find objectionable.

Chin Decl., Ex. G, ¶ 8.3. A subsequent section of the 2007 TOS provided that "[s]ome of the Services are supported by advertising revenue and may display advertisements and promotions" and that "[t]hese advertisements may be content-based to the content information stored on the Services, queries made through the Service or other information." *Id.* ¶ 17.1

The 2012 TOS deleted all of the above language and stated that users "give Google (and those [Google] work[s] with) a worldwide license to use . . ., create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), . . . and distribute such content." *Id.*, Ex. H. The 2013 TOS is, for purposes of the instant litigation, identical to the 2012 TOS. *Id.* ¶ 15 n.5.

Second, Google had in place several Privacy Policies during the class periods. The TOS referred users to the Privacy Policies. *Id.* ¶ 14. The Privacy Policies in effect from August 8, 2008, to October 3, 2010 stated that Google may collect "[i]nformation you provide, [c]ookies[,] [l]og information[,] [u]ser communications . . . to Google[,] [a]ffiliated sites, [l]inks[,] [and] [o]ther sites." *Id.*, Ex. I. Google described that it used such information for the purposes of "[p]roviding

our services to users, including the display of customized content and advertising." *Id*. In 2010, Google updated the Policy to state that the collected information would be used to "[p]rovide, maintain, protect, and improve our services (including advertising services) and develop new services." *Id*., Ex. K. Importantly, for all of these policies, under the heading of "User Communications," which Google collected, Google stated that "[w]hen you send email or other communications *to Google*, we may retain those communications in order to process your inquires, respond to your requests and improve our services." *Id.*, Exs. I-K. Google combined various product-specific Privacy Policies on March 1, 2012. The purpose of the combination was to allow Google to integrate user data collected from its various products.[3] In that Privacy Policy, Google eliminated the "User Communications" from the enumerated list of types of data that Google said it collected. *Id*., Ex. L.

Third, the Privacy Policies in place from August 7, 2008 to March 1, 2012 also incorporated product-specific privacy notices, such as two Gmail Privacy Notices that were in place until October 3, 2010. *Id.* ¶ 20; *id.*, Exs. M, N. The Gmail Privacy Notices stated that "Google records information such as account activity (including storage usage, number of log-ins), data displayed or clicked on (including UI [user interface] elements, ads, links); and other log information (including browser type, IP-address, date and time of access, cookie ID, and referrer URL)." *Id.* The Notices went on to state that "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."[4] *Id.*

---

[3] The change in the Privacy Policy is the subject of litigation pending before Magistrate Judge Grewal. *See In re Google, Inc. Privacy Policy Litig.*, No. 12-1382, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013).

[4] Google cites again, as it did in connection with the Motion to Dismiss, a "Legal Notice" that states that "Google does not claim any ownership in any of the content, including any text, data, information, images, photographs, music, sound, video, or other material, that [users] upload, transmit or store in [their] Gmail account." Chin Decl. ¶ 22; *id.*, Ex. O. The Notice further stated

Fourth, Google maintained a series of Help pages designed to provide users information on various subjects. *Id.* ¶ 24. The first of these pages, which was accessible through a link on the Create an Account" page that Gmail users utilized from June 2009 to June 2012, stated that "[i]n Gmail, ads are related to the content of your messages" and that "[a]d targeting in Gmail is fully automated and no humans read your email in order to target advertisements or related information." *Id.* ¶ 25; *id.*, Ex. P. Another Help page, titled "More on Gmail and Privacy," states that "[e]mail messages remain strictly between the sender and intended recipients" except in certain limited circumstances. *Id.*, Ex. R. "These exceptions include requests by users that Google's support staff access their email message in order to diagnose problems; when Google is required by law to do so; and when we are compelled to disclose personal information because we reasonably believe it's necessary in order to protect the rights, property or safety of Google, its users and the public." *Id.* The "More on Gmail and Privacy" Help page went on to state that "[i]n Gmail, users will see text ads and links to related pages that are relevant to the content of their messages." *Id.* A third Help page, titled "Gmail, Security & Privacy," states that "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." *Id.* ¶ 28. A fourth page, titled "Ads on Google search, Gmail, and certain other Google websites," states that "[w]hen we personalize ads, we display ads based on the contents of all your emails." *Id.* ¶ 30.

Fifth, Google maintained two other pages for short periods that contained information about targeted advertising. The first, a page titled "Privacy Center" that was available from July 2011 to June 2012, stated that "Google scans the text of Gmail messages in order to filter spam and detect viruses. The Gmail filtering system also scans keywords in users' email which are then used to match and serve ads." *Id.* ¶ 32. The second, a page titled "Your Data on Google: Advertising,"

---

that Google "will not use any of [users'] content for any purpose except to provide [users] with the service." *Id.*, Ex. O.

which was available from October 2011 to February 2013, stated that "[i]n Gmail, ads are related to the content of your messages." *Id.* ¶ 33.

Sixth, Google's Ad Preferences Manager, which was launched in 2009, had a webpage for "Ads on Search and Gmail" that stated that "[w]ith personalized ads, we can improve your ad experience by showing you ads related to websites you visit, recent searches and clicks, or information from your Gmail inbox." *Id.* ¶¶ 40, 42. Another webpage, "About Ads Settings" stated that "[t]he ads you see [in Gmail] may be based on many of the same factors as ads in Google Search as well as additional factors like the messages in your inbox." *Id.* ¶ 43. The webpage provided an example: "You've recently received lots of messages about photography and cameras. In Gmail, you may see an ad with a deal from a local camera store." *Id.*

Seventh, Google points to certain disclosures within the Gmail interface. *Id.* ¶ 54. Ads in Gmail are accompanied by a "Why this ad?" link, which when clicked displays a pop up that states that "[t]his ad is based on mails from your mailbox" and links to the Ads Preferences Managers discussed above. *Id.* ¶¶ 55-57. Moreover, from January 26, 2012 to March 1, 2012, Google advertised its new Privacy Policy on various Google websites and through a direct email to all Gmail users. *Id.* ¶¶ 48, 51. This email contained links to the TOS, Privacy Policy, Help pages, and Ad Preferences Manager. *Id.*, Ex. HH.

Eighth, Google cites blog posts and Securities and Exchange Commission ("SEC") filings as additional disclosures of its alleged interceptions of emails. *Id.* ¶ 34. A January 20, 2010 blog post on the Official Gmail Blog informed users that "[w]hen you open a message in Gmail, you often see ads related to that email. Let's say you're looking at a confirmation email from a hotel in Chicago. Next to your email, you might see ads about flights to Chicago." *Id.* ¶ 35. Moreover, Google cites one sentence of a more than one hundred page SEC filing, in which Google states that "[w]e serve small text ads that are relevant to the messages in Gmail." *Id.* ¶ 36.

United States District Court
For the Northern District of California

4. Disclosures to Cable One Users

As discussed above, Cable One contracted with Google and agreed to ensure that its end users agreed to the Google Apps TOS, which are, in all respects relevant to the instant litigation, identical to the 2007 Gmail TOS discussed above, which contained the language about Google's ability to pre-screen or review content for objectionable material. *Id.* ¶ 6. However, it is not clear from the record that Cable One's end users ever received a copy or link to the Google Apps TOS or that Cable One end users were required to agree to the TOS to create their accounts. That TOS states that "[b]y using Google's products, software, services, or web sites . . . , you agree to the following terms and conditions, and any policies, guidelines, or amendments thereto that may be presented to you from time to time, including but not limited to Program Policies and Legal Notices . . . ." *Id.*, Ex. C. The TOS also incorporates by reference the Privacy Policy in effect at the time, by linking to Google's Privacy Policy page, which contained the latest Privacy Policy. *Id.*

During the initial email migration process to Google Apps, Cable One provided users a link to the current version of the Google Privacy Policy (which contained the language that Google could collect "user communications . . . to Google") at the bottom of the Account Transfer page. *Id.*, Ex. OO. After the migration to Google Apps, from 2010 to at least 2011, Cable One's Self Support Portal page directed users interested in learning more about their email platform to Gmail Help pages. *Id.*, Ex. PP. The Gmail Help pages contain links to Google's Privacy Policy and TOS at the bottom of the page. *Id.* The Self Support Portal also provided a link to "Legal Notices" at the bottom of the pages, but it is unclear from the record where the "Legal Notices" link leads. *Id.*

5. Educational Institutions' Disclosures

As discussed above, the educational institutions with whom Google contracted were also required to obtain the necessary authorizations from end users for Google to provide its services. *Id.* ¶¶ 7-8. However, Google does not mandate how these educational institutions receive such authorizations, nor is that process uniform between various educational institutions. *Id.* ¶ 72. Accordingly, there are substantial differences between how each of the institutions approaches

disclosures. Moreover, it is unclear from the record what disclosures of the various universities each end user saw before registering for an account.

For example, for the University of the Pacific, the email sign-in page provides links to Google's Privacy Policy and TOS at the bottom of the page, below the sign-in button. ECF No. 107 ("Wong Decl.") ¶ 86. The University of Hawaii has a link to a Google Help Center to the side of the sign-in page. This Help Center contains links to Google's TOS and Privacy Policy. *Id.* ¶ 87. The Rochester Institute of Technology and Carnegie Mellon University direct users with questions regarding Google's processing of email to Google's Privacy Notices and Privacy Policies. *Id.* ¶ 89. As discussed above, the specific language of the TOS, Privacy Policies, and Privacy Notices have evolved over the last five years, but these universities provide links to the latest versions on Google's website. Therefore, some end users may have followed links from the universities to the TOS that contained the statement about Google's authority to pre-screen material to prevent objectionable content, while others may have viewed the Privacy Policies' discussion that Google was authorized to collect user communications to Google.

In contrast to the Google disclosures, some universities provide more detail to end users regarding the alleged interceptions at issue in the instant litigation. The University of California, Santa Cruz has a webpage titled "Security Information for Google Apps," where the University provides links to Google's TOS and Privacy Policies that were in effect at the time as discussed above. *Id.* ¶ 91. However, this webpage also contains a list of myths and facts about Gmail, one of which is particularly relevant here. *Id.*, Ex. 82. The webpage states, "MYTH: Google accesses people's email for marketing purposes" and "FACT: Google Apps for Education is ad-free for students, faculty, and staff. This means that your email is not processed by Google's advertising systems." *Id.* In contrast, the University of Alaska has a Google Mail FAQ page, which asks "I hear that Google reads my email. Is this true?" The answer states, "They do not 'read' your email per se. For use in targeted advertising on their other sites, and if your email is not encrypted, software (not a person) does scan your mail and compile keywords for advertising." *Id.* ¶ 88.

Similarly, Western Piedmont Community College's FAQ page states in response to the question "I've heard that Google scans the text in emails of Gmail accounts. Is that true?": "Well, yes, but probably not in the way you might be thinking. Google does use software or a 'bot' to scan Gmail emails for key words for the purposes of targeted advertising. Google then places small, unobtrusive, and relevant text ads alongside your Gmail messages, similar to those on the side of Google search results pages. The matching of ads to content is a completely automated process performed by computers. No humans read your email to target the ads, and no email content or other personally identifiable information is ever provided to advertisers." *Id.* ¶ 94. Stanford University's FAQ page links to Google's Privacy Policy and states that "[i]n order to provide essential core features for Stanford Alumni Email, Google runs completely automated scanning and indexing processes to offer spam filtering, anti-virus protection, and malware detection. Their systems also scan content to make sure Apps work better for users, enabling functionality like search in Gmail or Google Docs." *Id.*, Ex. 89.

6. Publicity Regarding Operation of Gmail

Google also points to media reports that discuss Google's scanning of emails as potential disclosures to which Class members may have been exposed. *Id.* ¶ 4. The news reports about Google's scanning practices fall broadly into four categories.

First, there was extensive media reporting of Gmail's launch in 2004. *Id.* ¶¶ 12-26. Several of the articles noted that Google automatically scanned all emails for the purposes of providing targeted advertising related to the content of emails. *Id.* For example, a USA Today article from 2004 states that "Google's computers automatically scan the body of messages for keywords used to tailor ads and match other information in its vast database." *Id.*, Ex. 4. A New York Times column stated that Google "said that its software would place ads in your incoming messages, relevant to their contents." *Id.*, Ex. 7. An article in the Chicago Tribune stated that "Google uses its AdSense software to read every word in every e-mail, and it then serves up related ads in the right margin." *Id.*, Ex. 11. Finally, a San Jose Mercury News article stated that "[t]he most controversial

aspect of the [Gmail] service will likely be the small text ads that Google will automatically place in every e-mail message. Powered by the company's AdSense program, the ads will be contextual, meaning they will relate to keywords in the e-mail." Wong Decl., Ex. 15.

Second, there was continued discussion in the media between 2005 and 2010 regarding Google's scanning practices. *Id*. ¶ 35. For example, a 2007 New York Times story about an unrelated online phone start-up, leads with "[c]ompanies like Google scan their e-mail users' in-boxes to deliver ads related to those messages. Will people be as willing to let a company listen in on their phone conversations to do the same?" *Id.*, Ex. 30. Similarly, a 2008 NPR story reported that "four years ago, when Google launched its ad-based Gmail, a lot of people were concerned that Google would be scanning private email to sell targeted ads. Today, most people don't seem to mind so much and continue to use it." *Id.*, Ex. 34. A 2008 Washington Post article notes that "[m]illions of people subject themselves to . . . intensive scrutiny when they use Google's Gmail service, which scans the text of each message to place more relevant ads." *Id.*, Ex. 35.

Third, there was news coverage of Google's 2011 roll out of a new advertising system, which allowed Google not only to present advertisements targeted to individual emails, but rather allowed Google to present advertisements tailored to information about users that Google aggregates over time. *Id.* ¶ 50. NBC News reported, for example, that "[w]hat if your email service gradually learned from the emails you send and read so that it could show you ads which you might actually be interested in? That's exactly what Google will be doing soon." *Id.*, Ex. 46. Similarly, PC World reported that "[f]or years, Gmail has been reading users' e-mails to display relevant ads, but soon it'll go a step further by learning users' habits." *Id.*, Ex. 47. A New York Times column also reported on this shift, stating that "[l]ast month, Google also announced that it was trying to make its ads even more 'useful and relevant' by scanning for 'importance signals' and recurring topics within messages to better serve up appropriate advertising."[5] *Id.*, Ex. 50.

[5] Google also cites publicity surrounding its 2012 consolidation of various Privacy Policies discussed above. Wong Decl. ¶ 60. However, coverage of this consolidation related principally to

Fourth, there has been media coverage of the instant litigation and related litigation. *Id.* ¶ 70. For example, an Associated Press article states that "[a] Pennsylvania woman has accused Google Inc. of illegal wiretapping for 'intercepting' emails she sent to Gmail accounts and publishing content-related ads. Her lawsuit echoes others filed around the country by class-action lawyers who say the practice violates wiretap laws in some states." *Id.*, Ex. 64. A CBS News article also reported on the instant litigation, stating that "[f]or years, Google's computers have scanned the content of millions of Gmails—Google's popular email service—in order to figure out what ads the user might respond to."[6] *Id.*, Ex. 67.

B. Procedural History

1. *Dunbar*

The first case that makes up this multi-district litigation, *Dunbar v. Google*, was filed on November 17, 2010, in the Eastern District of Texas. *See Dunbar v. Google, Inc.* ("*Dunbar I*"), No. 10-CV-194, ECF No. 1 (E.D. Tex. Nov. 17, 2010). After full briefing, on May 23, 2011, Judge Folsom denied in full Google's motion to dismiss Dunbar's complaint. *See Dunbar I*, ECF No. 61 (E.D. Tex. May 23, 2011). After the order on the motion to dismiss, the parties exchanged substantial discovery. *See Dunbar I*, ECF No. 87 (E.D. Tex. Aug. 17, 2011).

Dunbar then filed a motion for class certification. After full briefing and a hearing on December 8, 2011, Judge Folsom denied Plaintiffs' class certification motion without prejudice on March 16, 2012. *See Dunbar I*, ECF No. 156 (E.D. Tex. March 16, 2012). In the order denying class certification, Judge Folsom found that Dunbar had, on balance, satisfied the requirements of Rule 23(a): numerosity, commonality, typicality, and adequacy of class representative and class counsel. *Id.* at 10-16. However, Judge Folsom found that Dunbar's proposed class, of all non-

---

Google's sharing of information across services rather than to the scanning of emails. For example, a Wall Street Journal article states that "[t]he big difference here is that Google has previously not combined information from so many different services, instead of keeping some of it in 'silos' that were originally intended in part to preserve users' anonymity." *Id.*, Ex. 53.

[6] Google also cites an advertising campaign by Microsoft, which criticizes Google's record on privacy. Wong Decl. ¶¶ 64-69.

Gmail users who had sent emails from their non-"@gmail.com" accounts to a Gmail or Cable One account, was not ascertainable, because the proposed class excluded "individuals . . . who seek actual damages and profits from Google." *Id.* at 4. Judge Folsom found that this exclusion was not objective, and that accordingly, the class was not ascertainable. *Id.* at 9. Furthermore, Judge Folsom found that Dunbar's class definition was deficient because users with non-"@gmail.com" accounts necessarily included Google Apps users. *Id.* Judge Folsom also found that Dunbar had not satisfied Rule 23(b)(3)'s superiority requirement because Dunbar had not presented an adequate trial plan. *Id.* at 16-20. Finally, Judge Folsom found that Dunbar had not satisfied the predominance requirement because there would be potential individualized questions of consent under Dunbar's proposed trial plan. *Id.* at 21-22.

On April 20, 2012, one month after Judge Folsom's class certification denial, Google filed another motion to dismiss, seeking dismissal on venue grounds. *See Dunbar I*, ECF No. 160 (E.D. Tex. April 20, 2012). In the alternative, Google requested that the case be transferred to the Northern District of California. *See id.* The motion to transfer was granted, and the case was transferred to this Court and assigned to the undersigned judge on June 27, 2012. *See Dunbar v. Google, Inc.* ("*Dunbar II*"), No. 12-3305, ECF No. 180 (N.D. Cal. July 23, 2012).

On August 28, 2012, Dunbar moved for leave to amend the complaint and indicated his intent to file a renewed class certification motion. *See Dunbar II*, ECF No. 205 (N.D. Cal. Aug. 28, 2012). After full briefing and a hearing, this Court granted the motion for leave to amend on December 12, 2012. *See Dunbar II*, ECF No. 226 (N.D. Cal. Dec. 12, 2012). The Court found that Dunbar had been diligent since Judge Folsom's denial of the initial class certification motion, and that Google would not be unduly prejudiced by amendment because the Court would not reopen class discovery, which had closed on October 25, 2011. *Id.* at 17-25. Moreover, in the order on Dunbar's motion for leave to amend, the Court extensively addressed Google's contention that amendment would be futile because the amended complaint could not remedy the defects that Judge Folsom identified in his class certification order. *Id.* at 25-30. Specifically, the Court noted

that the new class definition in the complaint did not exclude those who sought damages from Google and that the new class definition focused on Cable One users rather than users with non-"@gmail.com" addresses, which would encompass Google Apps users. *Id.* at 26-27. Moreover, the Court noted that while predominance and superiority concerns may preclude class certification, leave to amend should be granted because Judge Folsom's denial of class certification was explicitly without prejudice, suggesting that amendment and more evidence could cure the deficiencies identified in Judge Folsom's class certification order. *Id.* at 28-30. After this Court granted leave, Plaintiff filed a Third Amended Complaint, which Google answered. *See Dunbar II*, ECF No. 228 (N.D. Cal. Dec. 14, 2013); *Dunbar II*, ECF No. 246 (N.D. Cal. Jan. 14, 2013).

On January 8, 2013, this Court set a briefing schedule for Dunbar's renewed class certification motion. *See Dunbar II*, ECF No. 242 (N.D. Cal. Jan. 8, 2013). Pursuant to this schedule, on January 28, 2013, Dunbar filed a renewed class certification motion. *See Dunbar II*, ECF No. 249 (N.D. Cal. Jan. 28, 2013). In the motion, Dunbar sought to certify a class of Cable One users who used their Cable One Google Apps email account to send a message to a Gmail user or receive a message in the two years before the filing of *Dunbar* up until class certification. *Id.* at 6. On March 7, 2013, Google filed an opposition, contending that Dunbar could not show predominance because individual issues of whether interceptions had taken place and individual issues of consent would predominate over any common issues, that Dunbar was an inadequate class representative, and that adjudication by class would not be superior to individualized adjudications. *See Dunbar II*, ECF No. 261 (N.D. Cal. March 7, 2013). Dunbar filed his reply brief on March 28, 2013, contending that both express and implied consent could be litigated on a class-wide basis, that Dunbar is an adequate class representative, and that class adjudication would be superior to individual actions. *See Dunbar II*, ECF No. 269 (N.D. Cal. March 28, 2013).

2. Other Cases and Consolidation

While *Dunbar* was pending, five other actions involving substantially similar allegations against Google were filed in this District and throughout the country. *See Scott, et al. v. Google*,

Inc., No. 12-3413 (N.D. Cal.); *Scott v. Google, Inc.*, No. 12-614 (N.D. Fla.); *A.K. v. Google, Inc.*, No. 12-1179 (S.D. Ill.); *Knowles v. Google, Inc.*, No. 12-2022 (D. Md.); *Brinkman v. Google, Inc.*, No. 12-6699 (E.D. Pa.). On April 1, 2013, before the Court could rule on Dunbar's class certification motion, the Judicial Panel on Multidistrict Litigation issued a Transfer Order, centralizing *Dunbar* along with the five other actions in the Northern District of California before the undersigned judge. *See* ECF No. 1. At an initial case management conference on April 18, 2013, the Court ordered Plaintiffs to file a consolidated complaint on May 16, 2013, set the briefing schedule for any motion to dismiss, and scheduled a hearing for September 5, 2013. *See* ECF No. 9. The Court also set a class certification briefing schedule and a class certification hearing for January 16, 2014.[7] *See id.* On May 6, 2013, this Court related a seventh action, *Fread v. Google, Inc.*, No. 13-1961 (N.D. Cal.), as part of this multi-district litigation. *See* ECF No. 29.

3. Motion to Dismiss and Motion to Certify

In line with the Court's scheduling order, Plaintiffs filed a Consolidated Complaint on May 16, 2013. *See* ECF No. 38. That complaint attempted to state causes of action under (1) ECPA; (2) CIPA; (3) Maryland's Wiretap Act; (4) Florida's Wiretap Act; and (5) Pennsylvania's Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701 (2012). Google filed a Motion to Dismiss the Consolidated Complaint on June 13, 2013. *See* ECF No. 44. After full briefing, this Court held a hearing on the Motion to Dismiss on September 5, 2013. *See* ECF No. 64.

The Court issued an Order Granting in Part and Denying in Part the Motion to Dismiss on September 26, 2013. *See* ECF No. 69. The Court granted Google's Motion with respect to Plaintiffs' claims under section 632 of the California Penal Code, finding that emails were not "confidential" under that part of CIPA. *Id.* at 40-42. The Court further found that Pennsylvania law did not confer anti-wiretapping protections on *recipients* of emails and therefore granted Google's Motion with respect to the Pennsylvania law claims of non-Gmail users who merely received

[7] The hearing was continued to February 27, 2014. *See* ECF No. 127.

emails from Gmail users. *Id.* at 42-43. The Court denied the rest of the Motion to Dismiss, rejecting Google's two principal bases for dismissal. First, the Court rejected Google's contention that any interceptions in the instant case fell within the "ordinary course" of Google's business and were therefore exempt from anti-wiretapping statutes. Utilizing the tools of statutory interpretation, the Court concluded that the ordinary course of business exception was intended only to protect electronic communication service providers from liability where the interceptions helped facilitate or were instrumental to the provision of the electronic communication service. *Id.* at 19-20 ("In light of the statutory text, case law, statutory scheme, and legislative history concerning the ordinary course of business exception, the Court finds that the ['ordinary course of business'] exception is narrow and designed only to protect electronic communication service providers against a finding of liability under the Wiretap Act where the interception facilitated or was incidental to provision of the electronic communication service at issue."). The Court further found that interceptions that violate an electronic communication service provider's internal policies, as was alleged in the instant case, could not be within the provider's ordinary course of business. *Id.* at 20-22. Second, the Court rejected Google's argument that all Gmail users had consented to the alleged interceptions based on the TOS and Privacy Policy. The Court concluded that the TOS and Privacy Policy did not provide sufficient disclosures to conclude that Gmail users had consented to the alleged interceptions. *Id.* at 22-26. The Court further rejected Google's contention that all email users, regardless of whether they had viewed any disclosures, had impliedly consented to the alleged interceptions, because all email users, including non-Gmail users, understand that such interceptions are part of how emails are transmitted. *Id.* at 27-28. The Court further held that Plaintiffs could proceed on their claims under section 631 of CIPA. *Id.* at 28-40.

On October 9, 2013, Google filed a Motion for § 1292(b) Certification for Interlocutory Review of this Court's September 26, 2013 Order on the Motion to Dismiss. *See* ECF No. 80. Plaintiffs opposed that motion on October 16, 2013. *See* ECF No. 83. This Court held a hearing on the Section 1292(b) Certification Motion on October 29, 2013. *See* ECF No. 94. On January 27,

2014, the Court entered an Order denying Section 1292(b) Certification Motion, because the long and tortured history of the *Dunbar* action and the consolidated multi-district litigation suggested that immediate appeal would not materially advance the termination of the litigation. *See* ECF No. 129. Specifically, the Court found that Google's desire to seek appellate review was belated, as Google did not seek appellate review of Judge Folsom's May 23, 2011 order denying the initial motion to dismiss. *Id.* at 3. Moreover, the Court concluded that appellate review, years after the initial complaint was filed, would not prevent the parties from expending substantial resources as "multiple motions to dismiss have been fully briefed, argued, and ruled upon; multiple motions for class certification have been fully briefed; class discovery had closed in one of the cases more than two years ago; and fact discovery on the merits is set to close in less than three months." *Id.* at 6. Finally, the Court agreed with Judge Folsom that regardless of where the precise line for the "ordinary course of business" exception was drawn, further factual development would be necessary and thus resolution of this issue was not appropriate on a motion to dismiss, which is limited to the four corners of the complaint. *Id.* at 6 n.2.

C. The Instant Motion

Plaintiffs filed the instant Motion for Class Certification on October 24, 2013. *See* Mot. In their Motion, Plaintiffs seek certification of the following four classes and three subclasses as described in the following chart:

Class Definition	Class Reps.	Class Periods	Statutes at Issue
Cable One users who have, through their Cable One accounts, sent an email to an "@gmail.com" or "@cableone.com" email address or have received an email. ("Cable One Class")	Dunbar	Two years prior to filing of the action to the date of certification.	Federal Wiretap Act
All Google Apps for Education users who have, through their Google Apps for Education accounts, sent an email to an "@gmail.com" address or have received an email. ("Education Class")	Fread and Carrillo	Longest period allowed by statute of limitations to the date of certification.	Federal Wiretap Act
All Gmail users between the ages of thirteen and the age of majority ("minors") who used their	A.K., as next of	Two years prior to filing of the	Federal Wiretap Act

Gmail accounts to send an email to a minor Gmail user or to receive an email from a non-Gmail user or a minor Gmail user. ("Minor Class")	friend to minor J.K.	action to the date of certification.	
All U.S. resident non-Gmail users who have used their non-Gmail accounts to receive an email from an "@gmail.com" address or to send an email message to an "@gmail.com" email address. ("Non-Gmail Wiretap Act Class")	Kovler, Harrington, Brad Scott	Longest period allowed by statute of limitations to the date of certification.	Federal Wiretap Act
Subclass of Non-Gmail Wiretap Act Class: All U.S. residents, except California residents, who have used their non-Gmail accounts to send an email message to an "@gmail.com" email address. ("Non-Gmail CIPA Subclass")	Kovler, Harrington, Brad Scott	Longest period allowed by statute of limitations to the date of certification.	CIPA
Subclass of Non-Gmail Wiretap Act Class: All Florida residents who have used their non-Gmail accounts to send an email message to an "@gmail.com" email address. ("Non-Gmail Florida Subclass")	Brent Scott	Longest period allowed by statute of limitations to the date of certification.	Florida Statute §§ 934.03, *et seq.*
Subclass of Non-Gmail Wiretap Act Class: All Maryland residents who have used their non-Gmail accounts to send an email message to an "@gmail.com" email address. ("Non-Gmail Maryland Subclass")	Knowles	Longest period allowed by statute of limitations to the date of certification.	Maryland Cts. and Judicial Proceedings Code §§ 10-402, *et seq.*

See Mot. at 9-10; Reply at 6 n.18; ECF No. 115. Excluded from all classes are all state, local, and federal government entities; individuals who timely opt out; current or former Google employees; individuals who have previously settled the claims identified in the FACC; and any currently sitting federal judge and people within three degrees of consanguinity to any federal judge. FACC ¶ 352. Defendants filed an Opposition to Plaintiffs' Motion for Class Certification on November 21, 2013. *See* Opp. Plaintiffs filed a Reply in support of their Motion on December 19, 2013. *See* Reply.[8] The Court held a hearing on February 27, 2014. *See* Tr.

[8] After the close of briefing, the parties filed motions to supplement the record. On February 6, 2014, Plaintiffs filed a Motion for Leave to Supplement the Record, which Google opposed. ECF Nos. 130-2, 134. Plaintiffs seek to introduce emails regarding the interceptions between named Plaintiff Fread and Google. The Court DENIES Plaintiff's motion on the basis that the emails go to Fread's individual concerns about the use of Google Apps services by the University of Hawaii and thus are not relevant to any issues of class certification. On February 25, 2014, Google filed a Motion to Supplement the Record with additional excerpts of a deposition of Plaintiffs' expert, Dr. Matthew Green, who submitted a declaration in conjunction with the Reply in support of the

II. LEGAL STANDARD

Federal Rule of Civil Procedure 23, which governs class certification, has two sets of distinct requirements that Plaintiffs must meet before the Court may certify a class. Plaintiffs must meet all of the requirements of Rule 23(a) and must satisfy at least one of the prongs of Rule 23(b).

Under Rule 23(a), the Court may certify a class only where "(1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a). Courts refer to these four requirements, which must be satisfied to maintain a class action, as "numerosity, commonality, typicality and adequacy of representation." *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 588 (9th Cir. 2012). Further, courts have implied an additional requirement under Rule 23(a): that the class to be certified be ascertainable. *See Marcus v. BMW of North America, LLC*, 687 F.3d 583, 592-93 (3d Cir. 2012); *Herrera v. LCS Fin. Servs. Corp.*, 274 F.R.D. 666, 671-72 (N.D. Cal. 2011).

In addition to meeting the requirements of Rule 23(a), the Court must also find that Plaintiffs have satisfied "through evidentiary proof" one of the three subsections of Rule 23(b). *Comcast Corp. v. Behrend*, 133 S. Ct. 1426, 1432 (2013). The Court can certify a Rule 23(b)(1) class when Plaintiffs make a showing that there would be a risk of substantial prejudice or inconsistent adjudications if there were separate adjudications. Fed. R. Civ. P. 23(b)(1). The Court can certify a Rule 23(b)(2) class if "the party opposing the class has acted or refused to act on

---

instant Motion. *See* ECF No. 141. The Court GRANTED this motion, which Plaintiffs do not oppose, at the hearing. Tr. 7:20. Google also moved to file a Statement of Recent Decision regarding the Marin County Superior Court's decision in *Diamond v. Google*, which Plaintiffs have opposed. *See* ECF Nos. 141-42. The Court DENIES Google's motion because the reasoned tentative decision of the Marin County Superior Court was superseded by a two-sentence order on the motion that stated only that the Court's rationale was placed on the record. On March 18, 2014, Plaintiffs filed another Motion to Supplement the Record. *See* ECF No. 156-2. The Court GRANTS this Motion because the material contained therein relates to the uniformity in Google's processing of emails, which is relevant to class certification.

grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). Finally, the Court can certify a Rule 23(b)(3) class if the Court finds that "questions of law or fact common to class members *predominate* over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3) (emphasis added).

"[A] court's class-certification analysis must be 'rigorous' and may 'entail some overlap with the merits of the plaintiff's underlying claim.'" *Amgen Inc. v. Conn. Ret. Plans and Trust Funds*, 133 S. Ct. 1184, 1194 (2013) (quoting *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2551 (2011)); *see also Mazza*, 666 F.3d at 588 ("'Before certifying a class, the trial court must conduct a 'rigorous analysis' to determine whether the party seeking certification has met the prerequisites of Rule 23.'" (quoting *Zinser v. Accufix Research Inst., Inc.*, 253 F.3d 1180, 1186, *amended by* 273 F.3d 1266 (9th Cir. 2001)). Nevertheless, "Rule 23 grants courts no license to engage in free-ranging merits inquiries at the certification stage." *Amgen*, 133 S. Ct. at 1194-95. "Merits questions may be considered to the extent—but only to the extent—that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied." *Id.* at 1195. Within the framework of Rule 23, the Court ultimately has broad discretion over whether to certify a class. *Zinser*, 253 F.3d at 1186.

III. DISCUSSION

Plaintiffs move to certify all four Classes and three Subclasses identified above as Rule 23(b)(3) damages classes. Google does not challenge Plaintiffs' position that the putative Classes meet the numerosity and commonality requirements. Instead, Google contends that none of the Classes satisfies the ascertainability, predominance, and superiority requirements. Google also challenges some of the Classes under choice of law principles and contends that some Classes cannot meet the adequacy and typicality requirements of Rule 23(a). The Court finds that none of the Classes can satisfy the predominance requirement. Accordingly, the Court does not reach

United States District Court
For the Northern District of California

Google's remaining contentions. The Court begins by setting forth the legal standard for predominance and then applies that standard to the four Classes and three Subclasses. After doing so, the Court concludes that individual issues regarding whether members of the various Classes consented to the alleged interceptions will predominate over common issues.

A. Legal Standard for Predominance

The predominance inquiry of Rule 23(b)(3) "tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation." *Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 623 (1997). Accordingly, the predominance analysis "focuses on the relationship between the common and individual issues in the case." *Wang v. Chinese Daily News, Inc.*, 737 F.3d 538, 545 (9th Cir. 2013) (internal quotation marks omitted); *see also In re Wells Fargo Home Mortgage Overtime Pay Litig.*, 571 F.3d 953, 958 (9th Cir. 2009) ("Whether judicial economy will be served in a particular case turns on close scrutiny of the relationship between the common and individual issues." (internal quotation marks omitted)).

Undertaking the predominance analysis requires some inquiry into the merits, as the Court must consider "how a trial on the merits would be conducted if a class were certified." *Gene And Gene LLC v. BioPay LLC*, 541 F.3d 318, 326 (5th Cir. 2008); *see also Zinser*, 253 F.3d at 1190 (noting that district courts must consider as part of the predominance analysis whether a manageable class adjudication can be conducted). Though the Court needs to consider the merits to determine whether the action can be litigated on a class-wide basis, the Supreme Court has cautioned that class certification is not an opportunity for the Court to undertake plenary merits inquiries. As the Supreme Court has stated, "[m]erits questions may be considered to the extent—but only to the extent—that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied." *Amgen Inc.*, 133 S. Ct. at 1195; *see also In re Whirlpool Corp. Front-Loading Washer Prods. Liab. Litig.*, 722 F.3d 838, 851 (6th Cir. 2013) (noting that merits inquiries at the class certification stage are limited to those necessary to resolving the question presented by Rule 23).

The Court's predominance analysis "entails identifying the substantive issues that will control the outcome, assessing which issues will predominate, and then determining whether the issues are common to the class, a process that ultimately prevents the class from degenerating into a series of individual trials." *Gene And Gene LLC*, 541 F.3d at 326; *see also In re New Motor Vehicles Canadian Exp. Antitrust Litig.*, 522 F.3d 6, 20 (1st Cir. 2008) ("Under the predominance inquiry, a district court must formulate some prediction as to how specific issues will play out in order to determine whether common or individual issues predominate in a given case." (internal quotation marks omitted)); *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1022 (9th Cir. 1998) (finding predominance "[w]hen common questions present a significant aspect of the case and they can be resolved for all members of the class in a single adjudication"). To meet the predominance requirement, "common questions must be a significant aspect of the case that can be resolved for all members of the class in a single adjudication." *Berger v. Home Depot USA, Inc.*, 741 F.3d 1061, 1068 (9th Cir. 2014) (internal quotation marks and alterations omitted).

Importantly, the predominance inquiry is a pragmatic one, in which the Court does more than just count up common issues and individual issues. Wright & Miller, *Federal Practice & Procedure* § 1778 (3d ed. 2005) (noting that "the proper standard under Rule 23(b)(3) is a pragmatic one, which is in keeping with the basic objectives of the Rule 23(b)(3) class action"). As the Seventh Circuit recently stated, "predominance requires a qualitative assessment too; it is not bean counting." *Butler v. Sears, Roebuck & Co.*, 727 F.3d 796, 801 (7th Cir. 2013). The Court's inquiry is not whether common questions predominate with respect to individual elements or affirmative defenses; rather, the inquiry is a holistic one, in which the Court considers whether overall, considering the issues to be litigated, common issues will predominate. *Amgen*, 133 S. Ct. at 1196.

B. Application of the Predominance Standard

The Court now applies these standards to the four Classes and three Subclasses. The Court begins by describing the underlying merits inquiry before turning to the question of how best to

conduct such an inquiry. *Id.* at 1191 ("[T]he office of a Rule 23(b)(3) certification ruling is not to adjudicate the case; rather, it is to select the 'metho[d]' best suited to adjudication of the controversy 'fairly and efficiently.'" (internal alterations omitted)).

The Wiretap Act, as amended by the ECPA, prohibits the interception of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1); *Joffe v. Google, Inc.*, No. 11-17483, 2013 WL 6905957, at *3 (9th Cir. Dec. 27, 2013). More specifically, the Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); *see id.* § 2520 (providing a private right of action for violations of § 2511). The Wiretap Act contains several exemptions that render interceptions lawful. *See* 18 U.S.C. § 2511(2)(a)-(h). Among these exemptions is an exemption for consent:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception 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). The state anti-wiretapping statutes at issue in the instant litigation contain consent exceptions that are similar but require all parties to the intercepted communication to have consented. *See* Fla. Stat. § 934.03(2)(d); Md. Code, Cts. & Jud. Proc. § 10-402(c)(3); 18 Pa. Cons. Stat. § 5704(4).[9]

The question of whether Class members have consented to the alleged interceptions has been central to this case since its inception. Specifically, the issue of whether email users consented to the alleged interceptions was at issue in all rounds of briefing on motions to dismiss, all three rounds of briefing on class certification, and the briefing on the motion for leave to amend. *See*

[9] The distinction between one-party consent and two-party consent is immaterial to the Court's analysis, because as discussed below, the issue of whether *any* email user (Gmail user, Google Apps end user, or non-Gmail user) consented to the alleged interceptions is a question fraught with individualized inquiries.

Dunbar I, ECF No. 13 (E.D. Tex Feb. 4, 2011); *Dunbar I*, ECF No. 23 (E.D. Tex. March 10, 2011); *Dunbar I*, ECF No. 61; *Dunbar I*, ECF No. 119 (E.D. Tex. Oct. 25, 2011); *Dunbar II*, ECF No. 210-3 (N.D. Cal. Sept. 18, 2012); *Dunbar II*, ECF No. 261; ECF No. 44 at 13-21; Opp. at 11-18. The consent exception remains one of the principal disputed issues in this case. In fact, both sides in discussing predominance in their briefing on the instant Motion focus heavily on the consent exception.[10] For the reasons stated below, the Court finds that individual issues of consent are likely to predominate over any common issues, and that accordingly, class certification would be inappropriate.

The Court begins by briefly describing the consent exemption. Courts have interpreted the consent exemption to encompass two different forms of consent. First, consent can be express. *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996). Second, in the alternative, consent can be implied in fact based on whether the surrounding circumstances demonstrate that the party whose communications were intercepted knew of such interceptions. *Id.* Regardless, consent must be actual, and not constructive. *In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003) ("Consent may be explicit or implied, but it must be actual consent rather than constructive consent."). Importantly, under the Wiretap Act, the statute pursuant to which the Cable One Class, Education Class, Minor Class, and Non-Gmail Wiretap Act Class bring claims, only one party to the intercepted communication needs to consent to render the interception lawful. 18 U.S.C. §

[10] In the briefs, the parties dispute whether the question of whether emails were intercepted pursuant to the Wiretap Act is a common question or an individual question. *See* Mot. at 18-20; Opp. at 18-22; Reply at 6-9. Plaintiffs contend that Google uniformly intercepts emails for COB processing. Google notes that there are a number of situations in which emails are not subject to COB processing. Opp. at 18-19. Only one of these situations—Google claims that Google Apps Administrators can configure their systems to avoid COB processing—would lead to individualized inquiries. Google relies exclusively on a declaration from a Google engineer for Google's claim that Google Apps Administrators can avoid COB processing. *See* ECF No. 106 ("Long Decl.") ¶ 3. Plaintiffs contend that this declaration contradicts the engineer's previous deposition and Google's recent representations to the media, and that therefore the declaration is a sham. Green Reply Decl. ¶ 10; ECF No. 156-2. The Court need not decide the question of whether the declaration is valid and therefore whether the question of interceptions is a class-wide question, because the Court finds that even if this question were a class-wide question, that common questions would be overwhelmed by individualized questions of consent as discussed below.

2511(2)(d). Therefore, the ultimate merits inquiry requires not only consideration of whether the Class members consented, but also whether their correspondents consented.[11] However, for the three state statutes at issue with respect to the three Subclasses, the merits inquiry requires both parties to consent. Accordingly, if either party to a communication did not consent, that would end the inquiry.

In the instant litigation, Google has marshaled both express and implied theories of consent. Accordingly, the Court turns to each of the two theories of consent and describes the legal standard that must be applied with respect to each, the Court's rulings regarding the two theories of consent at the Motion to Dismiss stage, and the evidence in the record that the parties will marshal going forward to prove the existence or absence of consent. The Court concludes, for the reasons stated below, that this evidence suggests that consent must be litigated on an individual, rather than class-wide basis. The Court will conclude by addressing Plaintiffs' contentions to the contrary.

1. Express Consent

Courts have consistently noted that individuals may expressly consent to the interception of their communications. *Pharmatrak*, 329 F.3d at 19; *Van Poyck*, 77 F.3d at 292; *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987). However, detailed discussion of the express consent exception to the Wiretap Act in the case law is relatively scant. Nevertheless, at the Motion to Dismiss stage, Google contended that Gmail users and all Google Apps end users had expressly consented to Google's alleged interceptions. For this proposition, Google relied on the various

[11] The Court does not separately discuss Minor Class members' consent for four reasons. First, the parties have cited no case law suggesting that minors cannot provide consent to interceptions of their communications under the Wiretap Act. Second, Plaintiffs rely exclusively on a California statute, Cal. Fam. Code § 6701, to contend that minors cannot consent. However, this provision relates to contract law. As discussed below, consent for purposes of contract law is distinct from consent for purposes of the Wiretap Act. Third, even if state contract law consent principles were to negate a minor's ability to consent under the Wiretap Act, there would be individual questions as to where the minor email senders and recipients reside and which state laws should apply. The nationwide Minor Class would therefore require several individual inquiries even under Plaintiffs' theory. Fourth, to the extent that minors have corresponded with adults, there would be several individualized issues regarding the adult correspondent's consent, as discussed below.

TOS and Privacy Policies that were in effect between 2008 and 2013. In the Order on the Motion to Dismiss, this Court rejected Google's contentions. The Court held that the TOS and Privacy Policies did not provide sufficient disclosures regarding the alleged interceptions—the scanning of emails for the purposes of providing targeted advertising and creation of user profiles—to warrant dismissal under the express consent exception to the Wiretap Act. ECF No. 69 at 24-26. Specifically, the Court found that Google's reliance on the language of its TOS, which stated that "Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service," was misplaced because that provision related to Google's participation in the email delivery process to preclude objectionable content, particularly in light of the sentence that followed, which stated that "[f]or some of the Services, Google may provide tools to filter out explicit sexual content." *Id.* at 24.

Similarly, the Court was not persuaded that the Privacy Policies, which stated that Google collected "[i]nformation you provide, [c]ookies[,] [l]og information[,] [u]ser communications . . . to Google[,] [a]ffiliated sites, [l]inks[,] [and] [o]ther sites" and used such information for the purposes of "[p]roviding our services to users, including the display of customized content and advertising," provided clear enough disclosures regarding Google's interceptions of emails between users to provide targeted advertisements. *Id.* at 25. In fact, the Court found that certain statements in the Privacy Policies, which stated that Google would collect "user communications . . . *to Google*" could actively obscure Google's interceptions. *Id.*at 25-26 (emphasis in original).

At the instant stage of litigation, the Court must consider whether express consent is an issue that can be decided on a class-wide basis or whether individual issues will predominate. The Court notes that the question of express consent is usually a question of fact, where a fact-finder needs to interpret the express terms of any agreements to determine whether these agreements adequately notify individuals regarding the interceptions. *See Murray v. Fin. Visions, Inc.*, No. 07-2578, 2008 WL 4850328, at *4 (D. Ariz. Nov. 7, 2008).

Plaintiffs contend that the question of express consent is a question particularly susceptible to class-wide adjudication, since all Gmail users were subject to the same disclosures. While the Court agrees that express consent may be a common question with respect to the Minor Class and the Cable One Class, the express consent of Education Class members is likely to require individualized inquiries. This is so because Google had no single policy that required all Google Apps Administrators to provide the same disclosures to end users. *See* Chin Decl. ¶ 3. This means that the end users received vastly different disclosures depending on with which educational institution they were affiliated. Some institutions' disclosures are quite explicit. For example, Western Piedmont Community College tells its users that "Google does use software or a 'bot' to scan Gmail emails for key words for the purposes of targeted advertising." Wong Decl., Ex. 85. Similarly, the University of Alaska states that "For use in targeted advertising on [Google's] other sites, and if your email is not encrypted, software (not a person) does scan your mail and compile keywords for advertising." *Id.*, Ex. 79. Meanwhile, other universities, such as the University of the Pacific, merely incorporate Google's disclosures by citing to the TOS and Privacy Policies. *Id.*, Ex. 74. As discussed above, it is not clear that end users even had to look at these disclosures before they could create their accounts. Further, even if the users had seen these disclosures, as this Court noted above and in its Order on the Motion to Dismiss, Google's disclosures were vague at best, and misleading, at worst. For example, the TOS stated only that Google retained authority to pre-screen content to prevent objectionable material, while the Privacy Policies suggested only that Google would collect user communications *to Google*. Accordingly, the diversity of disclosures made by educational institutions, ranging from specific disclosures about the method and reasons for interceptions to the incorporation of vague disclosures, may well lead a fact-finder to conclude that end users at some universities consented, while end users at other universities did not. As such, the Court finds that there are substantial individualized inquiries on the issue of express consent.

In sum, the Court finds that with respect to the Education Class, the substantial individual questions regarding the nature of each Google Apps Administrator's disclosures are likely to lead

to individual questions regarding express consent that will predominate over common questions. The Court need not determine whether class-wide express consent questions will predominate over individual questions with respect to the Minor Class, Cable One Class, and the Non-Gmail User Classes because, as discussed below, the Court finds that individualized questions regarding implied consent will overwhelm any common issues regarding these Classes.

2. Implied Consent

The Court now turns to implied consent. Implied consent is an intensely factual question that requires consideration of the circumstances surrounding the interception to divine whether the party whose communication was intercepted was on notice that the communication would be intercepted. *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) ("It is the task of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception exceeded that consent."); *see also Murray*, 2008 WL 4850328, at *4 ("The question of consent, either express or implied, is often a fact-intensive inquiry and may vary with the circumstances of the parties."). As the D.C. Circuit has concluded, "[w]ithout actual notice, consent can only be implied when *the surrounding circumstances* convincingly show that the party knew about and consented to the interception." *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (internal quotation marks and alterations omitted; emphasis added); *Van Poyck*, 77 F.3d at 292 ("Consent may be express or may be implied in fact from *surrounding circumstances indicating that the defendant knowingly agreed to the surveillance*." (internal quotation marks and alterations omitted; emphasis added)). "[I]mplied consent is consent in fact which is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance." *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990) (internal alterations and quotation marks omitted).

Applying this standard to the Motion to Dismiss, which examines only the four corners of the complaint, the Court rejected Google's contention that the Court should conclude that all email users impliedly consented to Google's interceptions on the basis of the Complaint alone, because

all email users understand that such interceptions are part and parcel of the email delivery process. ECF No. 69 at 27. The Court found that there was no authority to support Google's "far-reaching proposition" that consent could be implied so broadly as a matter of law without any factual development. *Id.* The Court therefore concluded that accepting Google's theory of implied consent "would eviscerate the rule against interception" since under Google's theory, consent could easily be implied as a matter of law with respect to large swaths of electronic communication services. *Id.*

Now, at the class certification stage, the Court must consider what evidence Google can use to argue to the finder of fact that email users have impliedly consented to these interceptions. Google contends that a broad swath of evidence that email users were notified of the interceptions, such as Google disclosures, third-party disclosures, and news articles, are relevant to the factual question of implied consent. Plaintiffs contend that only Google's own disclosures to its users are relevant to the question of implied consent.

The Court agrees with Google. As discussed above, 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. For example, the First Circuit has suggested that whether a party has impliedly consented is a factual question that requires a close examination of all the circumstances:

> The 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. And the ultimate determination must proceed in light of the prophylactic purpose of [the Wiretap Act]—a purpose which suggests that consent should not casually be inferred.

Griggs-Ryan, 904 F.2d at 117. Accordingly, "consent can be limited based upon the 'subtleties and permutations inherent in a particular set of facts.'" *Shefts v. Petrakis*, 758 F. Supp. 2d 620, 631 (C.D. Ill. 2010) (quoting *Griggs-Ryan*, 904 F.2d at 119).

Amen is instructive. There, the Second Circuit found that the consent exception to the Wiretap Act applied in the context of inmates whose phone calls were recorded. *Amen*, 831 F.2d at

378-79. The Second Circuit found that consent could be implied, because the inmates were on notice from several sources that their phone calls were being recorded. *Id.* at 379. The Second Circuit found implied consent based on the following: (1) the taping system was discussed at inmates' orientation; (2) inmates received a handbook that discusses the interceptions; (3) there were notices near the phone alerting inmates of the monitoring; and (4) one of the inmate's case managers presented the inmate with a form containing a written notice of disclosures, which the inmate refused to sign. *Id.* The Second Circuit's reliance on a form that the inmate did not sign, but nevertheless saw, indicates that all materials to which an individual has notice are relevant to consent, not just contractual agreements. *See Van Poyck*, 77 F.3d at 292 (approvingly citing *Amen*).

The First Circuit's decision in *Williams v. Poulos*, 11 F.3d 271 (1st Cir. 1993), is in accord. There, the First Circuit affirmed a district court's finding, after a bench trial, that the CEO of a company had not consented to interceptions of his telephone calls by his employer. *Id.* at 281-82. The First Circuit noted that though the CEO was informed that the company had a system for randomly monitoring calls, it was not clear whether the CEO knew "(1) of the manner—i.e., the intercepting and recording of telephone conversations—in which this monitoring was conducted; and (2) that he himself would be subjected to such monitoring." *Id.* at 281. The First Circuit concluded:

> There was testimony tending to indicate that [the CEO] was so informed, which the district judge apparently chose not to credit, and testimony tending to indicate that he was not. In our view, the latter testimony, far from being incredible, was highly plausible. Thus, there is no basis for us to conclude that the district court clearly erred in finding that [the CEO] was not told of the manner in which the monitoring was conducted and that he himself would be monitored.

Id. at 281-82. The First Circuit, though ultimately rejecting the testimony, found that testimony about what the CEO knew was relevant to whether the CEO had consented. The First Circuit could have rejected the company's contentions out of hand by requiring official or written notice. Rather, the First Circuit found that the question of implied consent was fundamentally a factual question on which all the testimony regarding what the CEO knew was relevant. In light of these authorities,

the Court concludes that while consent may only be implied in a narrow set of circumstances, a broad set of materials are relevant to determining whether such consent should be implied.

Applying these legal principles here, the Court finds that individual issues regarding consent are likely to overwhelmingly predominate over common issues. Specifically, 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. First, Class members could have learned of the interceptions from various Google sources. For example, the "About Ads on Search, Gmail and across the web" page, which has been viewed more than a million times, states that "[t]he ads you see [in Gmail] may be based on many of the same factors as ads in Google Search as well as additional factors like the messages in your mailbox" and provides the following example: "You've recently received lots of messages about photography and cameras. In Gmail, you may see an ad with a deal from a local camera store." Chin Decl. ¶¶ 41, 43; *id.*, Ex. DD. Furthermore, the link for "Why This Ad?" next to each targeted advertisement in Gmail, which led users to the disclosure that "[t]his ad is based on emails from your inbox," was clicked thousands of times in every day. *Id.* ¶ 56; *id.*, Ex. JJ. Second, Class members may have learned about the alleged interceptions from various media sources.[12] For example, a 2004 Houston Chronicle article states that "some industry watchers have complained that Google scans account holders' messages for keywords and then delivers text-based ads relevant to the keywords detected. However, most Gmail users said they're not bothered by it." Wong Decl., Ex. 13. Along a similar note, a Washington Post article stated, "Google's Gmail service has generated some controversy among privacy activists for the way its technology serves up text ads to users based on the content of their messages. None of the Gmail account

[12] Plaintiffs contend that these third-party documents are impermissible hearsay. *See* Reply at 5 n.15. However, Google does not cite this material for the truth of the matter asserted therein—that is, to establish that Google actually intercepted emails. Rather, these documents are cited for the effect on the listener—that is, to show that Plaintiffs had knowledge that Google engaged in interceptions. *United States v. Payne*, 944 F.2d 1458, 1472 (9th Cir. 1991).

holders or would-be account holders contacted for this article expressed concerns along these lines." *Id.*, Ex. 9.

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.

3. Plaintiffs' Contentions

Plaintiffs make three arguments in support of their claim that consent can be determined on a class-wide basis. First, Plaintiffs contend that in determining whether Gmail users impliedly consented, the finder of fact should be limited to looking at a uniform set of Google's own disclosures, rather than to disclosures of third parties. Second, Plaintiffs contend that the parol evidence rule precludes the finder of fact from looking outside the contractual agreements between Gmail users and Google. Third, Plaintiffs contend that the specific disclosures to which Google points do not demonstrate consent, because those disclosures pre-date Google's shift in email delivery processing from the CAT2 Mixer (which scanned emails only when the emails were opened) to COB (which scans all emails while the emails are in transit). In essence, Plaintiffs' contention is that the third-party disclosures on which Google relies cannot disclose interceptions that did not exist at the time of the third-party disclosures.[13] The Court does not find any of these contentions persuasive for the reasons stated below.

[13] Plaintiffs also contend that consent can be negated on the basis that Google's interceptions were for the "purpose of committing [a] . . . tortious act in violation of the . . . laws of the United States

United States District Court
For the Northern District of California

First, Plaintiffs contend that the factual inquiry with respect to implied consent should be limited to looking at the disclosures that Google itself made, rather than disclosures that third parties, such as news media, made. Even if Plaintiffs were correct regarding the scope of documents to which a fact-finder could look, there would be a myriad of individual issues with respect to consent, because Google itself had several disclosures, which could not have been uniformly viewed by Class members. For example, as discussed above, a Google page titled "About Ads on Search, Gmail and across the web" stated that "[t]he ads you see [in Gmail] may be based on many of the same factors as ads in Google Search as well as additional factors like the messages in your inbox," and provided the following example: "You've recently received lots of messages about photography and cameras. In Gmail, you may see an ad with a deal from a local camera store." Chin Decl. ¶ 43, *id.*, Ex. DD. It is undisputed that this page has been viewed more than 1.6 million times since July 2012. *Id.* A finder of fact could conclude that Class members who viewed this particular disclosure were on notice of the alleged interceptions. Similarly, some Class members may have been part of the 100,000 individuals who clicked the "Why This Ad?" link next to a content-based advertisement in a single day. *Id.*¶ 58. Those users would have received a notice that "[t]his ad is based on emails from your inbox," which again, a fact-finder could find sufficient to imply consent. *Id.*, Ex. JJ. In light Google's own disclosures' diversity, even accepting

---

or any State," 18 U.S.C. § 2511(2)(d), and that this is a class-wide question. Mot. at 23-24. Google responds that Plaintiffs have failed to allege or provide any evidence that Google acted with the wrongful intent necessary to fall within the tort or crime exception to the consent exception. Opp. at 17. The Court agrees with Google. Alleged interceptions fall within the tort or crime exception only where the "primary motivation or a determining factor in [the interceptor's] actions has been to injure plaintiffs tortiously." *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 518 (S.D.N.Y. 2001) (internal quotation marks omitted). Nothing in the FACC, the briefing on the instant Motion, or the record suggests that this is Google's motivation here. Moreover, as the *DoubleClick* Court found in a different context, the tort or crime exception cannot apply where the interceptor's "purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money." *Id.* The same is true here. Accordingly, the tort or crime exception to the consent exception will be unavailing for Plaintiffs to show absence of consent. Therefore, individualized inquiries will be needed to determine what each Class member knew.

Plaintiffs' theory, a fact-finder would have to evaluate whether consent could be implied from the specific set of *Google* disclosures that each individual user encountered.

Second, the Court also sees no basis as to why the disclosures relevant to a fact-finder's determination of implied consent should be limited exclusively to Google disclosures. As discussed above, courts have held that the question of implied consent turns on whether the party whose communications were intercepted had notice of the interception or consented to the interception based on *all* of the surrounding circumstances. *Berry*, 146 F.3d at 1011; *Griggs-Ryan*, 904 F.2d at 117; *Amen*, 831 F.2d at 378. Plaintiffs do not cite any authority limiting the sources from which such notice or knowledge can be acquired, nor could this Court find such authority. Accordingly, the Court concludes that the full panoply of disclosures, from the news media, from Google, and from other sources, is relevant to the question of whether consent to the alleged interceptions should be implied from the surrounding circumstances. Plaintiffs contend that relying on extrinsic evidence outside of Google's agreements with Class members would violate the parol evidence rule or that consideration of such evidence would be prohibited by the merger clause in the TOS. While these could be valid contentions if Plaintiffs stated a breach of contract cause of action, these are not viable arguments with respect to the consent under the Wiretap Act, which requires the fact-finder to consider all the surrounding circumstances to determine whether an individual knew that her communications would be intercepted. *Amen*, 831 F.2d at 378 (holding that the critical question with respect to implied consent is whether consent can be implied "in fact from surrounding circumstances indicating that the [plaintiffs] knowingly agreed to the surveillance").

Plaintiffs rely exclusively on a Northern District of Illinois case, *Harris v. comScore, Inc.*, 292 F.R.D. 579, 585 (N.D. Ill. 2013), for their proposition regarding the parol evidence rule. The Court, however, finds *Harris* unpersuasive. The *Harris* court held that "ComScore [the intercepting entity] contends that the scope of consent will vary for each plaintiff depending on his subjective understanding of the agreement and the surrounding circumstances. In support, comScore notes that at least under the ECPA, consent need not be explicit, but can also be implied from the

surrounding circumstances. But that rule has no place where a party manifested consent through the adoption of a form contract." *Harris*, 292 F.R.D. at 585 (internal citations omitted). For the proposition in the last sentence, however, *Harris* merely cited a Seventh Circuit case interpreting Illinois contract law. The *Harris* court did not address the long line of cases that suggest a broader swath of materials is relevant to implied consent under the Wiretap Act. This Court concludes that unlike Illinois contract law, under which the subjective intent of the parties must give way to the terms of the contract that embody the parties' mutual assent, *see Nat'l Prod. Workers Union Ins. Trust v. Cigna Corp.*, 665 F.3d 897, 901 (7th Cir. 2011), the question of implied consent to interceptions prohibited by the Wiretap Act necessarily requires an inquiry into what the party whose communications were intercepted subjectively understood.

Moreover, *Harris*, even if applicable, is distinguishable. In *Harris*, the user had a direct contract with the service provider, in which the user must have agreed to the user licensing agreement before she could use the software that engaged in the alleged interceptions. *Id.* at 582 ("The consumer must check either 'Accept' or 'Decline' before he may click 'Next' to proceed with downloading the free digital product. OSSProxy will download and install on the consumer's computer only if the consumer checks 'Accept.'" (internal citations omitted)). In contrast, here, neither the Cable One nor Education Class members (who are end users) had any direct contractual relationship with Google. Moreover, in *Harris*, unlike this case, there were no potential other sources of disclosure, such as news articles, to which Class members in the instant litigation could have been exposed.

Furthermore, Plaintiffs' contention that a finder of fact may only look to the agreements between Google and its users in determining consent improperly collapses express and implied consent. The agreements between Google and its users define the scope of the universe of material that the Court may consider in determining whether Plaintiffs have *expressly consented.* If the fact-finder were limited to the same material for purposes of determining implied consent, then express and implied consent would be coterminous. Courts have recognized, however, that express and

implied consent are analytically distinct. *Berry*, 146 F.3d at 1011 (noting that even "*[w]ithout actual notice*," consent can be implied "when the surrounding circumstances convincingly show that the party knew about and consented to the interception" (emphasis added; internal citations and alterations omitted)). It is only logical, in light of this recognition, for a finder of fact to be allowed to consider a broader set of materials in answering the factual question of whether users impliedly consented to the interceptions.[14]

Finally, Plaintiffs raised a new theory at the hearing on the instant Motion to contend that consent was a common question. Specifically, Plaintiffs contended that the existence of various third-party disclosures is irrelevant, because these disclosures could not have alerted Class members to the method of interceptions. Plaintiffs rely on the fact that in [redacted] 2010, the Google device that intercepted emails shifted from the CAT2 Mixer, [redacted], to the COB, which scans all emails [redacted]. Plaintiffs contend that the pre-[redacted] 2010 third-party disclosures could have only alerted Class members about CAT2's processing, not COB's.

The Court is not persuaded. To find implied consent, a fact-finder need not determine email users had specific knowledge of the particular devices that intercepted their emails. Rather, the fact-finder need only be convinced based on the surrounding circumstances that email users were notified of interceptions. *Berry*, 146 F.3d at 1011 (noting that "[t]he key question in [the implied consent] inquiry obviously is whether parties were given sufficient notice" of the interceptions). To be relevant to this factual inquiry, a disclosure does not need to provide the specific devices at

[14] Plaintiffs' reliance on the deposition testimony of Google's 30(b)(6) witness on consent, Aaron Rothman, is misplaced. Plaintiffs rely on Mr. Rothman's testimony in response to counsel's question regarding how an average user would know that Google interprets words in emails for meaning that "it is very clear in—in the multitude of documents provided by Google." Mot. at 21 (citing Rommel Decl., Ex. I ("Rothman Depo.") at 298). Plaintiffs overread Mr. Rothman's testimony. In that part of Mr. Rothman's testimony, he was merely contending that Google's policies are sufficient to establish express consent. He was not, as Plaintiffs suggest, contending that the documents provided by Google were the sole sources from which users could learn of Google's alleged interceptions.

issue. *Griggs-Ryan*, 904 F.2d at 117 ("The 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."). Rather, a fact-finder could find implied consent even based on broad disclosures. Therefore, the Court finds that Google may rely on news articles to argue to the finder of fact that users impliedly consented, even if those news articles do not recite the specific devices that are alleged to have intercepted Class members' emails.

Even if the Court were to accept Plaintiffs' contention that the *pre-*[redacted] 2010 disclosures could not have alerted users to COB processing, which did not exist at that point, the Court would still conclude that individualized questions predominate with respect to consent because of the panoply of *post-*[redacted] 2010 disclosures that could be found to have put Class members on notice. For example, a 2012 Wall Street Journal article regarding Google's consolidation of Privacy Policies informed users that "you may have noticed ads in your Gmail based on emails you had typed. Those appear because Google scans the content of emails for things like keywords that may be relevant for advertising." Wong Decl., Ex. 53. Similarly, an October 22, 2012, New York Times article about Microsoft's privacy policies states that "[t]he Microsoft policy appeared to give the company the same rights as Google, which scans the content of e-mails sent through its Gmail system, focusing on keywords to generate advertising that it thinks will interest the user." *Id.*, Ex. 55. Therefore, even if *pre-*[redacted] 2010 disclosures were not relevant to the implied consent inquiry, the Court would conclude that the *post-*[redacted] 2010 disclosures give rise to numerous individual inquiries regarding individual Class members' knowledge of the interceptions. Plaintiffs' sole contention with respect to these post-[redacted] 2010 disclosures is that these disclosures could not have disclosed COB processing, because Google has stated that the operation of the COB is a trade secret. The Court finds, however, that even if these disclosures did not specifically name COB processing, a fact-finder could conclude that these disclosures are sufficient surrounding circumstances to imply that email users "knowingly agreed

to the surveillance," that is, the interceptions of their emails for purposes of targeted advertisements and user profiles. *Amen*, 831 F.2d at 378.

C. Conclusion Regarding Predominance

In sum, the Court finds that a fact-finder would have to determine to what disclosures each Class member was exposed and whether such disclosures were sufficient to conclude, under the Wiretap Act, that Class members consented to the alleged Google interceptions of email. This factual inquiry is an intensely individualized one. Furthermore, the myriad disclosures among the various Google Apps for Education Administrators raise a variety of individualized questions regarding express consent for the Education Class. The individualized questions with respect to consent, which will likely be Google's principal affirmative defense, are likely to overwhelm any common issues. Therefore, the Court cannot conclude that Plaintiffs have met their burden of demonstrating that the proposed Classes satisfy the predominance requirement.

This Court's conclusion that Plaintiffs fail to demonstrate predominance is consonant with *Murray v. Fin. Visions, Inc.*, No. 07-2578, 2008 WL 4850328 (D. Ariz. Nov. 7, 2008). *Murray* concerned a Wiretap Act claim brought by a putative class of employees, who sold securities and other investment products, against their employer, a broker-dealer and investment advisor. *Id.* at *1. The employees had contracted with a website hosting service approved by the employer for website and email services. *Id.* The employer asked the website hosting service to intercept and automatically transmit all email sent from or received by any employees to the employer. *Id.* The *Murray* court denied class certification, finding that individual issues predominate with respect to consent. *Id.* at *4. The court held that "[t]he question of consent, either express or implied, is often a fact-intensive inquiry and may vary with the circumstances of the parties." *Id.*

The individualized nature of the consent inquiry in the instant case is even clearer than that in *Murray*. In *Murray*, the sole source of disclosures, whether from the employer or from other sources, was the SEC regulation and the *Murray* court found that there would be individualized inquiries regarding the impact of that regulation on employees' knowledge and conduct. In

United States District Court
For the Northern District of California

contrast, here, there are many more disclosures, from Google itself and from the news media, which were unlikely to be uniformly viewed by members of the putative Classes. Accordingly, the Court finds that individualized issues of consent would overwhelm any individual questions.

IV. CONCLUSION

For the foregoing reasons, the Court DENIES Plaintiffs' Motion for Class Certification. In one sentence on the last page of Plaintiffs' Reply brief, Plaintiffs request to refile their Motion for Class Certification if this Court were to deny the instant Motion so that Plaintiffs may seek certification of a Rule 23(b)(2) class seeking injunctive relief. *See* Reply at 20, n.52. The Court rejects Plaintiffs' request. Plaintiffs have briefed Class Certification three times, and class discovery closed in *Dunbar* on October 25, 2011. *Dunbar II*, ECF No. 226, at 3. To the extent that Plaintiffs intended to seek class certification under any theory, Plaintiffs should have done so in the instant Motion. Moreover, Plaintiffs could have requested an opportunity to refile in their Motion, but only sought such relief at the end of their Reply. *See United States v. Romm*, 455 F.3d 990, 997 (9th Cir. 2006) (noting that the Court need not consider arguments raised for the first time in the Reply). Entertaining Plaintiffs' belated request would prejudice Google, which has been opposing class certification motions in this litigation since September 2011, and which did not have the opportunity in the briefing on the instant Motion to oppose Plaintiffs' request to refile. Moreover, the Court finds that when asked about Plaintiffs' request to refile at the hearing, Plaintiffs' counsel did not provide any persuasive basis for allowing such refiling. Tr. 61:15-63:18. Accordingly, the denial of the Class Certification Motion is with prejudice.

IT IS SO ORDERED.

Dated: March 18, 2014

Lucy H. Koh

LUCY H. KOH
United States District Judge