COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
WHITTY SOMVICHIAN (194463)
(wsomvichian@cooley.com)
KYLE C. WONG (224021)
(kwong@cooley.com)
101 California Street, 5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

Attorneys for Defendant
GOOGLE INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE GOOGLE INC. GMAIL LITIGATION

Case No. 5:13-md-02430 LHK (PSG)

EXHIBIT A TO DECLARATION OF STACEY KAPADIA IN SUPPORT OF DEFENDANT GOOGLE INC.'S ADMINISTRATIVE MOTION TO FILE PORTIONS OF DOCUMENTS UNDER SEAL

Judge: Hon. Lucy H. Koh
Dept: Courtroom 8 – 4th Floor

[PUBLIC REDACTED VERSION]

Exhibit A

REDACTED VERSION OF DOCUMENTS SOUGHT TO BE SEALED

COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
WHITTY SOMVICHIAN (194463)
(wsomvichian@cooley.com)
KYLE C. WONG (224021)
(kwong@cooley.com)
101 California Street, 5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

Attorneys for Defendant
GOOGLE INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE GOOGLE INC. GMAIL LITIGATION

Case No. 5:13-md-02430 LHK (PSG)

DEFENDANT GOOGLE INC.'S OPPOSITION TO PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

Date: January 16, 2013
Time: 1:30 p.m.
Dept.: Courtroom 8 - 4th Floor
Judge: Hon. Lucy H. Koh

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

OTHER AUTHORITIES

I. INTRODUCTION.

Plaintiffs' Class Certification Motion ("Motion") seeks to amalgamate an unprecedented (and ultimately unascertainable) collection of individuals into a series of classes to challenge the automated scanning of email—a practice has been an openly disclosed and widely discussed part of Google's Gmail service since its inception nearly a decade ago. Collectively, Plaintiffs' proposed classes would indiscriminately amass together virtually everyone in the United States with a non-Gmail email account, along with large groups of the over 400 million people who use Gmail and Google Apps. Plaintiffs' proposed classes would encompass individuals who are well aware of the automated scanning in Gmail and have no objection to it (or who actively benefit from the features it enables); people whose emails were never scanned at all; people who send or receive commercial emails and do not expect (or even want) their emails to be private; spammers, fraudsters, and others who send emails to Gmail users for abusive purposes; and others who have no viable claim yet would be swept up in Plaintiffs' effort to criminalize the core aspects of Google's free Gmail service. While Plaintiffs' ambition in seeking to certify these massively overbroad classes is not lacking, the legal and evidentiary support they offer to justify certification certainly is.

Plaintiffs' class certification theories have multiple defects, but the most glaring is the complete failure to present any viable proposal for addressing the necessary elements of their claims on a classwide basis. First, Plaintiffs make no showing that they can resolve the critical issue of implied consent on a class-wide basis. Instead, they recycle the same arguments, previously rejected in the *Dunbar* matter (ECF No. 156), that consent can be resolved by assessing Google's disclosures in a vacuum while ignoring the actual knowledge of the individuals involved in the emails at issue. Established law, however, requires a fact-finder to assess *all* relevant circumstances to determine if a party to a communication consented to the practices at issue—*not* simply whether a set of disclosures is objectively reasonable in the abstract. Accordingly, for each one of the many billions of emails implicated in this case, a fact-finder would need to assess whether the senders and recipients were aware of the automatic scanning in Gmail based on an immense array of individualized evidence, including thousands of

public disclosures (from both Google and non-Google sources) that have publicized Gmail's automated processes since 2004. This is a Herculean task beyond the resources of the Court and parties.

Second, Plaintiffs also offer no method for analyzing the untold number of emails at issue to identify those that involved the alleged wrongful scanning they seek to challenge. Instead, Plaintiffs skirt the issue entirely by asking the Court to assume that *all* emails are uniformly scanned without exception. This assumption is demonstrably false. Indeed, Plaintiffs and their counsel are well aware of the numerous exceptions in which scanning is *not* applied, but have opted to ignore the undisputed record and present a facade of uniformity they hope will seem more amenable to certification. Plaintiffs should not be allowed to certify a class based on a fiction of uniform processing that ignores how the Gmail system actually works and the many user- and email-specific factors on which Plaintiffs' claims depend.

Plaintiffs' Motion also fails for a host of additional reasons, including (1) the massive overbreadth of the proposed classes, which encompass large swaths of individuals with no legal standing; (2) the failure to propose any feasible method to ascertain the individuals who meet the proposed class definitions; and (3) the inadequacy of the individual Plaintiffs, whose testimony demonstrated a glaring lack of oversight over the litigation and whose atypical circumstances disqualify them from acting as class representatives. Any of these issues alone would be fatal, and collectively they pose an insurmountable and incurable obstacle to class certification.

For all these reasons, Google respectfully requests that the Court deny Plaintiffs' Motion in its entirety as to all claims and all proposed classes.

II. BACKGROUND.

A. Plaintiffs' Allegations, Proposed Classes, and Deposition Testimony.

As the Court is aware, Plaintiffs' claims all derive from the core allegation that Google's automated scanning of emails in the Gmail system is illegal. Plaintiffs' Motion focuses in particular on the processing implemented by the [redacted]. Both processes are involved in displaying ads to Gmail users based on a user's emails. The [redacted] also implements a number of other Gmail features, like automatically categorizing emails

to help users organize their inboxes, identifying dates in an email to create clickable links for users to create calendar entries, among many others. (Declaration of S. Kapadia ("Kapadia Decl."), ¶ 17.) Information from the [redacted] is also used in spam detection, which Plaintiffs concede is an appropriate form of scanning. (*Id.* ¶ 21.) Plaintiffs' Motion further refers to the creation of "user profiles" as a separate wrongful practice. But contrary to these vague assertions, the [redacted] is simply part of the process of showing targeted ads in Gmail.[1] (*Id.* ¶ 26.)

The individual plaintiffs, their claims, and proposed classes are summarized below:

Named Plaintiff	**Email Account**	**Claims**	**Proposed Classes**
Dunbar	Google Apps account through CableOne	ECPA (18 U.S.C. §2510, *et seq.*)	All CableOne users who sent an email to a Gmail or Cable One user, or received an email message in their account
Fread	Google Apps for Education account through Univ. of Hawaii	ECPA	All U.S. Google Apps for Education Users who sent an email to a Gmail user or received an email message in their account
Carillo	Google Apps for Education account through Univ. of Pacific	ECPA	Same as Fread
J.K.	Gmail	ECPA	All Minor U.S. Gmail Users who sent or received an email from a non-Gmail user or another minor Gmail User
Kovler, Harrington, Brad Scott	Non-Gmail	ECPA CIPA (Cal. Penal Code § 631)	ECPA Class: All U.S. Non-Gmail Users who received an original email from a Gmail user or sent an email to a Gmail user and received a reply CIPA Class: Same as above but excluding California residents
Knowles	Non-Gmail (also uses Gmail)	Maryland wiretapping law	Maryland Non-Gmail Users who received an original email from, or sent an email to, a Gmail User[2]
Brent Scott	Non-Gmail	Florida wiretapping law	Florida Non-Gmail Users who received an original email from, or sent an email to, a Gmail User

Plaintiffs Dunbar, Fread, Carrillo, and J.K. are referred to collectively as the "Gmail Plaintiffs" and their proposed classes are collectively the "Gmail Classes." The other plaintiffs

[1] Plaintiffs allude to other Gmail systems like the [redacted] as "intercepting devices." (Mot. at 4.) Plaintiffs do not explain how these systems could be illegal "devices"; nor do they present evidence to show that they are applied on a uniform basis for class certification purposes. To the contrary, these processes fall far beyond the scope of Plaintiffs' wiretapping claims, as explained in the Kapadia Declaration. (Kapadia Decl., ¶¶ 23-26.)

[2] Given the overlap among the CIPA, Maryland, and Florida classes, Plaintiffs seem to be claiming that Maryland and Florida residents can seek a triple recovery under (1) their home state wiretapping laws, (2) CIPA, and (3) ECPA. This result highlights the need to apply a single state law to each claimant based on their state of residency, as discussed below in Section III.E.

are collectively the "Non-Gmail Plaintiffs" and their proposed classes are the "Non-Gmail Classes." Plaintiffs Kovler, Harrington, and Brad Scott are also referred to as the "CIPA Plaintiffs" and they seek to represent the "CIPA Class."

Notably, none of the Plaintiffs (save one) took any steps to pursue any claims regarding Gmail before counsel or employees of counsel actively reached out to them to participate in the litigation. (*See, e.g.*, Declaration of Whitty Somvichian ("Somv. Decl."), ¶¶ 17, 38, 49, 65, 88.) Moreover, all Gmail Plaintiffs have continued to use their accounts and reap the benefits of Google's free services even *after* filing their complaints complaining of Google's practices. (*Id.* ¶¶ 4, 19, 32, 52.) One even opened a new Gmail account after filing his Complaint. (*Id.* ¶ 53.) Similarly, all Non-Gmail Plaintiffs continued to correspond with Gmail users after filing their complaints. (*Id.* ¶¶ 39, 67, 81, 89, 98.) None of the Plaintiffs took any actions to alert others, including their immediate family members, to stop using Gmail or to stop emailing with Gmail users, despite their claims of dire privacy intrusions in the Gmail system. (*Id.* ¶¶ 19, 34, 41, 55, 67, 81, 89, 98.) Additional facts about these Plaintiffs are discussed below in Section III.F.

B. Google's Terms and Disclosures.

To use Gmail or Cable One's Google Apps service, users must affirmatively agree to Google's Terms of Service ("TOS") and the incorporated terms, including Google's Privacy Policy. In addition to the terms the Court previously considered on Google's Motion to Dismiss, the TOS also incorporated a Gmail-specific Privacy Policy (not referenced in Plaintiffs' Complaint) which explained (among other disclosures) that "[t]he Gmail service includes relevant advertising and related links based on … [the] *content of messages* and other information related to your use of Gmail." (Declaration of B. Chin ("Chin Decl."), Ex. M; emphasis added.)

In addition to these contractual terms, Google provides a variety of disclosures explaining that the Gmail system scans email content to deliver targeted ads and for other purposes. These disclosures are detailed in the accompanying Chin Declaration and include the following:

- At certain times, the "Create an Account" page that users accessed to create a Gmail account explained that in "Gmail, you won't see blinking banner ads. Instead, ***we display ads you might find useful that are relevant to the content of your messages***." (*Id.* Ex. F (emphasis added).)

- When a Gmail user views an email, the ads shown are accompanied by a link titled **"Why this ad?"** Clicking the link causes a pop-up window to appear that explains "***This ad is based on emails from your mailbox***" and links to further disclosures. (*Id*. Ex. JJ (emphasis added); Somv. Decl., ¶ 51.)

- Google also maintains a publicly accessible "Help Center" with information on Gmail, which explained during the class period that:

  "***[A]utomatic scanning and filtering technology is at the heart of Gmail***. ***Gmail scans and processes all messages*** using fully automated systems in order to do useful and innovative stuff like filter spam, detect viruses and malware, show relevant ads, and develop and deliver new features across your Google experience." (Chin Decl., Ex. S (emphasis added).)

- Google's website also explains: ***"In Gmail, ads are related to the content of your messages***. Our goal is to provide Gmail users with ads that are useful and relevant to their interests. Ad targeting in Gmail is fully automated, and no humans read your email in order to target advertisements or related information. ***This type of automated scanning is how many email services, not just Gmail, provide features like spam filtering and spell checking***." (*Id*. Ex. P (emphasis added).)

These are just a sampling of the available disclosures, which have been in place throughout the class period and have been viewed by many millions of people over time. (*Id*. ¶¶ 26, 41, 43, 53.)

C. Additional Publicity Surrounding Gmail's Scanning Processes.

Thousands of *non*-Google sources have also discussed and publicized the automated scanning of emails in Gmail since its launch in 2004. (These are detailed in the Declaration of Kyle Wong ("Wong Decl."), filed herewith.) Gmail's launch was extensively covered by the media at the time, with numerous stories focusing on the automated scanning used to serve targeted ads. For example, a New York Times article explained that Google uses "software" to "place ads in your incoming messages, relevant to their contents," and further opined that privacy concerns were "overblown" because "no human ever looks at the Gmail e-mail. Computers do the scanning . . . just the way your current e-mail provider scans your messages for spam and viruses . . . If Gmail creeps you out, just don't sign up. That would be a shame, though, because you'd be missing a wonderful thing." (*See* Wong Decl., Ex. 7.) In the six-month period spanning Gmail's launch, there were hundreds of similar articles referring to the scanning of emails in the Gmail system. (Wong Decl., ¶¶ 6-7, Exs. 2-19.) In the years since, there have been thousands more stories on Gmail-related subjects in a variety of media channels, including television, radio, and the most widely read newspapers and periodicals in the country. (*Id*. ¶¶ 8-9, Exs. 20-73.)

Notably, the comments posted in the online versions of these articles show that many individuals are well aware of the automated scanning in Gmail and have no issue with it. (*Id.* ¶¶ 31, 46, 51, 56, 59, 62, Exs. 24, 37, 44, 49, 52, 54, 57, 68.)

Due to the initial novelty of Gmail's advertising feature, California State Senator Liz Figueroa publicly announced in 2004 that she was proposing a bill to address Google's automated scanning. (*Id.* ¶ 28, Ex. 20.) The Legislature ultimately dropped this proposed bill. (*Id.* ¶ 29, Ex. 21.) California's Attorney General was also urged to investigate whether Google's scanning violates the CIPA statute at issue in this case. The Attorney General promised to investigate but also chose not to take any action. (*Id.* ¶ 30, Ex. 23.) These legislative and investigative processes served to heighten and extend awareness of Google's Gmail practices.

Ongoing publicity has also been driven by Google's competitors and critics. One example is a widely disseminated anti-Google ad campaign by Microsoft, which highlights the automated scanning used to deliver ads in Gmail. (*Id.* ¶¶ 64-69, Exs. 56-60.) In addition, numerous privacy advocates and plaintiffs' lawyers–*including the lawyers in this case*–have publicized Google's practices, presumably as a way to attract clients. (*Id.* ¶¶ 70-82, Ex. 61-73.) For example, the Arnold law firm publicized this case on its website and provided links to a video from Fox News and an ABC News report that discuss Gmail's automated email scanning. (*Id.* ¶ 75, Exs. 65-66.)

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

D. Individual Emails Are Not Processed In A Uniform Manner.

Contrary to Plaintiff's blanket assertion, the scanning of emails in the Gmail system is *not* "uniform." (Mot. at 3.) To the contrary, whether an email undergoes a particular scanning process depends on numerous individualized factors, as detailed in the Kapadia Declaration. For example, the scanning implemented by the [redacted] is *not* applied to emails that [redacted] (Kapadia Decl., ¶¶ 18-19.) Similarly, the [redacted] process is only applied to emails in specific circumstances depending on [redacted], among other factors. (*Id.* ¶ 10.)

[redacted] emails opened on a mobile device do not include ads and are [redacted]. (*Id.*) Despite Plaintiffs' repeated assertions of "uniform" scanning, these exceptions are confirmed throughout the record, including the very evidence Plaintiffs submitted in support of their Motion.[3] (*See* Stewart Decl., ¶¶ 4-6, 8-12, 14.)

Importantly, senders of emails (whether Gmail users or non-Gmail users) have no data in their own email accounts that could be used to determine if the emails they send to Gmail users are scanned by the automated systems that Plaintiffs seek to challenge. (Kapadia Decl., ¶¶ 11, 20.) This entirely undermines the claims process that Plaintiffs propose as the sole method of ascertaining the proposed classes and identifying the instances of alleged wrongful scanning, as discussed below.

III. ARGUMENT

A. Class Certification Standards.

A class action is "an exception to the usual rule that litigation is conducted by and on behalf of the individual named parties only." *Comcast v Behrend*, 133 S. Ct. 1426, 1432 (2013) (quotations omitted). To come within the exception, a plaintiff "must affirmatively demonstrate his compliance" with Rule 23 and satisfy the Court, based on "a rigorous analysis," that the prerequisites of certification are satisfied. *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2551 (2011) (quotations omitted). Under *Dukes*, commonality under Rule 23(a) requires a "common contention" that "is capable of classwide resolution" and "will resolve an issue that is central to the validity of each one of the claims in one stroke." *Id.* Commonality is measured by "the capacity of a classwide proceeding to generate common *answers* apt to drive the resolution of the litigation." *Id.* In assessing these requirements, "[d]issimilarities within the proposed class are what have the potential to impede the generation of common answers." *Id.* Where, as here, a plaintiff relies on Rule 23(b)(3), the Supreme Court has noted that "Rule 23(b)(3)'s predominance criterion is even more demanding than Rule 23(a)." *Comcast*, 133 S. Ct. at 1432. Because Rule

[3] Plaintiffs take testimony out of context to suggest that Google witnesses have testified incorrectly about the scanning of outgoing emails. (*See* Somv. Decl. ¶¶ 103-07.) But the purported discrepancies are the result of imprecise questions directed at Google's complex systems for transmitting emails. Google discovery responses have repeatedly explained the circumstances in which a sent email can be scanned for advertising purposes. (*Id.* ¶¶ 108-09.)

23(b)(3) "is designed for situations in which class-action treatment is not as clearly called for," courts must "take a 'close look' at whether common questions predominate over individual ones." *Comcast*, 133 S. Ct. at 1432 (quotations omitted). Plaintiffs' Motion fails for multiple reasons under these standards.

B. Plaintiffs' Proposed Classes Are Unascertainable And Overbroad.

As an initial matter, the proposed classes are not ascertainable under Rule 23 because:

> The method of determining whether someone is in the class must be "administratively feasible." A plaintiff does not satisfy the ascertainability requirement if individualized fact-finding or mini-trials will be required to prove class membership. "Administrative feasibility means that identifying class members is a manageable process that does not require much, if any, individual factual inquiry."

Carrera v. Bayer Corp., 727 F.3d 300, 307-08 (3d Cir. 2013). *See also Tietsworth v. Sears, Roebuck & Co.*, No. 5:09-cv-00288-JF(HRL), 2013 WL 1303100, at *3-4 (N.D. Cal. Mar. 28, 2013) (denying certification where "ascertaining class membership would require unmanageable individualized inquiry") (quotations omitted).

Far from being "administratively feasible," any attempt to ascertain the Non-Gmail Classes would—under Plaintiffs' own proposal—require first sending email notice to *all* "non-Gmail users with addresses in Google's email system" in what would likely be the largest email notice campaign ever undertaken in litigation. (Mot. at 12.)[4] Plaintiffs never explain how they intend to implement this unprecedented notice campaign. And even if it were feasible, the parties would then need to (1) receive and review individual evidence from potentially millions of claimants to confirm that they meet the specific requirements of the various class definitions, and (2) resolve an untold number of disputes regarding this mass of submissions—just to identify the individuals who might meet the proposed class definitions and setting aside the myriad issues needed to resolve their claims. These problems undermine Plaintiff's entire Motion because

[4] Plaintiffs are forced to rely on this claims process because there is no existing data *within Google* that could be used to identify the proposed classes. For example, Google has no data that could reliably be used (1) to identify if someone who communicates with a Gmail user resides in a particular state, or (2) to show that an email sent by a Gmail user to a non-Gmail user was received by the intended recipient, as required under the definitions of the Non-Gmail Classes. Nor does Google have an existing list of all non-Gmail email accounts that have been used over time to send emails to, or receive emails from, the Gmail system. (*See* Kapadia Decl. ¶¶ 38-39.)

Plaintiffs propose to apply this individualized claims process for *all* classes. (*See* Mot. at 11.)

Even in cases involving substantially smaller classes and fewer issues, courts have denied certification where identifying the class members required this sort of individual claims process. *See Carrera*, 727 F.3d at 309 (affirming denial of certification and rejecting plaintiffs' contention that "the class is ascertainable using affidavits of class members" to identify purchases of the disputed product); *Tietsworth*, 2013 WL 1303100, at *3-4 (denying certification and rejecting plaintiff's argument that "identifying information [regarding the disputed products] could be used to check each Machine during a claim procedure"); *Xavier v. Philip Morris USA Inc.*,787 F. Supp. 2d 1075, 1089 (N.D. Cal. 2011) (rejecting proposal to ascertain the class based on class member affidavits). Certification should be denied for the same reasons here, given the inevitable quagmire of individual litigation that would result from Plaintiffs' notice and claims proposal.

C. The Proposed Classes Are Overbroad And Improper.

Even if the proposed class members could be identified, the result would be a massively overbroad collection of individuals, many of whom have no injury or colorable claim. Under established Ninth Circuit precedent, "'no class may be certified that contains members lacking Article III standing.'" *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 594 (9th Cir. 2012). In *Mazza*, the Court held (in a consumer fraud claim) that "the relevant class must be defined in such a way as to include *only* members who were exposed to advertising that is alleged to be materially misleading. The relevant class *must also exclude* those members who learned of the [alleged omissions] before they [engaged in the disputed transactions]." *Id.* at 596 (emphases added). *See also Mazur v. eBay Inc.*, 257 F.R.D. 563, 567 (N.D. Cal. 2009) (denying certification of case involving deceptive auctions where "the class as currently defined would include … non-harmed auction winners," making the proposed class "imprecise and overbroad").

Plaintiffs' proposed classes violate this basic rule because they would indiscriminately sweep into the litigation large swaths of individuals who have no conceivable right of recovery against Google, including:

- Countless individuals who used Gmail or corresponded with Gmail users after seeing one of the thousands of sources explaining the automated scanning in the Gmail system—persons who would fall within the consent exceptions of the claims at issue

(as further discussed below).

- Individuals (like several of the Plaintiffs) who have a non-Gmail email account *and* a Gmail account, who fall within the Non-Gmail Classes but are bound to Google's terms that authorize Google to apply user information for purposes of providing Google services (*see* Chin Decl., ¶¶ 9, 13-15)[5];
- Individuals whose emails were never scanned by the alleged "devices," who have no conceivable claim (as discussed below).
- Individuals who sent spam, computer viruses, or other abusive (or illegal) emails to Gmail users, who cannot use the wiretapping statutes to benefit from their own wrongful conduct.[6]
- Individuals who send or receive commercial emails that are not protected by the wiretapping statutes at issue.[7]

The Court should not certify proposed classes that are comprised in large part of these individuals (and others) who have no individual right to pursue a claim against Google. *See above*; *see also Diacakis v. Comcast Corp.*, No. C 11-3002 SBA, 2013 WL 1878921, at *4 (N.D. Cal. May 3, 2013) (denying certification and explaining that "[s]ince the proposed class includes persons who were not injured in the same manner as Plaintiff, the proposed class is overbroad.").

D. Individual Issues Overwhelmingly Predominate.

In addition to these defects, Plaintiffs' claims cannot be certified given the overwhelming predominance of individual issues that cannot feasibly be litigated on a classwide basis.

---

[5] Hundreds of millions of Gmail users have designated a non-Gmail account as a secondary method of contact, showing that a large portion of the Non-Gmail Class in fact consists of Gmail users bound to Google's terms. (Chin Decl., ¶ 11.) In addition, the Non-Gmail Classes could be construed to include users of Google Apps, who are also potentially bound to terms that permit Google to apply scanning. (*See* Somv. Decl., ¶¶ 110-13.)

[6] Even if Plaintiffs purport to include these persons in the class, Google would be entitled to defend against their claims on multiple grounds requiring individualized litigation. For example, Google may have a counterclaim against those who sent commercial emails in violation of the federal CAN-SPAM Act, 15 U.S.C. § 7701 *et seq*., § 7706(g)(1). Google would also be entitled to defend itself based on general principles of unclean hands. *See Kendall-Jackson Winery, Ltd. v. Super. Ct.*, 76 Cal. App. 4th 970, 978 (1999) ("The [unclean hands] doctrine demands that a plaintiff act fairly in the matter for which he seeks a remedy. He must come into court with clean hands … or he will be denied relief, regardless of the merits of his claim.").

[7] By excluding business entities from their class definitions, Plaintiffs concede that commercial communications are not protected by the wiretapping statutes. The same limitation should bar claims by individuals who send commercial emails for business purposes and have no expectation or desire that their messages will remain private (which would be impossible to identify absent individual review). (*See* Somv. Decl., ¶ 59 (attaching Plaintiff testimony agreeing that claims do not encompass commercial or other emails with no expectation of privacy.)

1. Plaintiff Cannot Litigate The Issue of Consent On a Classwide Basis.

Critically, for all of the claims at issue, each class member must demonstrate that the alleged "interceptions" occurred without consent.[8] In applying this exception, "consent need not be explicit but may be implied from the surrounding circumstances." *Medina v. Cnty. of Riverside*, 308 F. App'x 118, 120 (9th Cir. 2009). Implied consent does not require that someone subjectively approve of the alleged "interception," as Plaintiffs suggest. Rather, implied consent applies whenever the circumstances show that someone uses a method of communication knowing his or her communications will be "intercepted" by a third-party. *See id.*[9]

Courts look to a broad array of evidence to resolve implied consent, including:

(1) Whether an individual saw written disclosures of the disputed practice. *See United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996).

(2) Whether an individual received non-written explanations. *Griggs-Ryan v. Smith*, 904 F.2d 112, 117-19 (1st Cir. 1990).

(3) Whether an individual was aware of online privacy policies related to the disputed practices. *See People v. Nakai*, 183 Cal. App. 4th 499, 518 (2010) (assessing whether a party was aware of Yahoo!'s privacy policy in determining whether the party impliedly consented to the recording of his online chat messages under CIPA);

(4) Whether an individual was familiar with the disputed practices based on the circumstances of his or her employment. *See Shefts v. Petrakis*, 758 F. Supp. 2d 620, 631 (C.D. Ill. 2010) (assessing implied consent based on corporate officer's experience and knowledge).

(5) Whether an individual was aware of general industry practices involving email and online communications. *See, e.g., State v. Townsend*, 57 P.3d 255, 260 (Wash. 2002) ("To be available for reading or printing, the [email] message first must be recorded on another computer's memory.… [An email sender] thus implicitly consents to having the message recorded on the addressee's computer.").

Given the highly individualized inquiry needed to resolve implied consent, courts have consistently denied certification of wiretapping claims. In *Medina*, the Ninth Circuit affirmed

[8] Multiple courts have held that a plaintiff must prove lack of consent under the Wiretap Act. *See, e.g., United States v. Wuliger*, 981 F.2d 1497, 1503 (6th Cir. 1992). Even if Google bears the burden of proving consent, it would not affect the class certification analysis because "individual issues necessary to decide an affirmative defense may preclude class certification." *Gene & Gene LLC v. BioPay LLC*, 541 F.3d 318, 327 (5th Cir. 2008) (quotations omitted).

[9] Plaintiffs claim that Google admitted that the issue of consent is a "common issue" in other briefing. (Mot. at 15.) This refers to Google's motion to the MDL Panel, in which Google noted that the individual cases now consolidated with this Court share common fact allegations regarding the operation of the Gmail system. (*See* ECF No. 238 at 1-2, Ex. A.) This has nothing to do with whether the claims of *individual class members* can be resolved from common facts.

denial of certification of a class of prisoners who claimed that defendants violated ECPA by recording their communications without consent. 308 F. App'x at 120. The Court first found that implied consent applied to the individual plaintiffs because they had seen disclosures "alert[ing them to] the risk of wiretapping." *Id.* Because the same type of individual analysis would be needed for each class member, the Court held that "common questions do not predominate since [determining liability] would require intense individual examinations . . . ." *Id.* Similarly, in *Murray v. Financial Visions, Inc.*, No. CV–07–2578-PHX-FJM, 2008 WL 4850328, at *4 (D. Ariz. Nov. 7, 2008), the court declined to certify a class of employees who claimed their emails were intercepted under ECPA, explaining 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…. Accordingly, defendants' liability under the Wiretap Act will require an individualized showing of each class member's knowledge and consent with respect to each intercepted email." *Id.* at *4.[10] Numerous courts have reached the same conclusion in other contexts.[11]

[10] Other courts have denied certification of claims brought under state analogues to ECPA. *See also, e.g., Schwartz v. Dana Corp./Parish Div.*, 196 F.R.D. 275, 284-85 (E.D. Pa. 2000); *Kline v. Sec. Guards, Inc.*, 196 F.R.D. 261, 272-74 (E.D. Pa. 2000).

[11] *See Gene & Gene*, 541 F.3d at 329 (denying certification of claim under the Telephone Communications Privacy Act ("TCPA") where plaintiffs had failed to demonstrate a "sensible method of establishing consent or the lack thereof via class-wide proof"); *Jones v. Corbis Corp.*, 815 F. Supp. 2d 1108, 1117 (C.D. Cal. 2011) (denying certification of right of publicity claim because the consent issues were "highly individualized and depend[ed] on the circumstances surrounding each photograph"); *Balthazor v. Cent. Credit Servs., Inc.*, No. 10-62435-CIV, 2012 WL 6725872, at *4 (S.D. Fla. Dec. 27, 2012) (denying certification because TCPA claim "would necessarily involve an individual assessment of whether each class member consented to receive telephone calls on their cellular telephone."); *Vigus v. S. Ill. Riverboat/Casino Cruises, Inc.*, 274 F.R.D. 229, 235-38 (S.D. Ill. 2011) (denying certification where plaintiff had no method to identify which class members consented to phone calls); *Conrad v. Gen. Motors Acceptance Corp.*, 283 F.R.D. 326, 330 (N.D. Tex. 2012) (denying certification in TCPA case because "the consent issue would necessitate individual inquiries regarding each putative classmember's account and the circumstances surrounding each call …."); *Hicks v. Client Servs., Inc.*, No. 07–61822–CIV, 2008 WL 5479111, at *8 (S.D. Fla. Dec. 11, 2008) (denying certification in TCPA case because "consent is an issue that would have to be determined on an individual basis at trial"); *Arch v. Am. Tobacco Co.*, 175 F.R.D. 469, 490-91 (E.D. Pa. 1997) (denying certification where consent defense turned on individual questions involving "the subjective knowledge and behavior" of each class member); *Hanni v. Am. Airlines, Inc.*, No. C 08-00732 CW, 2010 WL 1576435, at *6 (N.D. Cal. Apr. 19, 2010) ("The issue of consent is individual [and] . . . precludes a finding that common issues predominate.")

a. Resolving consent will require individualized examinations that cannot be applied on a classwide basis.

The implied consent issues here are vastly *more* complex than those which precluded certification in the cases above, because a fact-finder would need to assess the knowledge of *each* sender and *each* recipient for *each* one of the billions of emails potentially at issue. This is an impossible task on its face.

First, a fact-finder would need to assess whether the senders and recipients for each email were aware of the automated scanning in Gmail based on the broad array of information available from Google.[12] For example, implied consent could apply based on the public Help page explaining that "automatic scanning and filtering technology is at the heart of Gmail" and "Gmail scans … *all* messages" for various purposes including "show[ing] relevant ads…." (Chin Decl., Ex. S (emphasis added).) In litigating a claim over any individual email, Google would be entitled to show that implied consent applies to someone who was aware of this disclosure and continued to use Gmail or correspond with Gmail users despite knowing that "Gmail scans … all messages." (*Id*.) This is just one among dozens of Google disclosures that would need to be considered, as detailed in the Chin Declaration.[13]

A fact-finder would also need to address whether the senders and recipients were exposed to a myriad of *non*-Google sources, as detailed in the Wong Declaration. For example, the consent exception would potentially apply to anyone who was aware of the legislative and regulatory inquiries during the 2004 launch of Gmail, which specifically addressed the use of automated scanning to show targeted ads (and which resulted in no action). Or anyone who has read the news in the nine years since the rollout of Gmail and seen one of the thousands of articles discussing the automated scanning features of Gmail (as discussed above). Or anyone, like Mr. Fread, who was aware of the extensive press coverage relating to both the pending Gmail

[12] Google's public disclosures are equally accessible to Gmail users and non-Gmail users.

[13] With respect to Gmail users in particular, a fact-finder would also need to assess the additional information available in each user's Gmail account. For example, the consent defense could apply to Plaintiff J.K. based on his admission that he clicked on the "Why This Ad?" link associated with the ads in his Gmail account and read the explanation that "***This ad is based on emails from your mailbox.***" (*See* Somv. Decl., ¶ 51.)

litigation and other privacy cases in the courts. (*See* Somv. Decl., ¶ 28.) Or anyone who has seen public materials from the various consumer organizations that monitor and scrutinize Google's Gmail practices. Or anyone who has been exposed to advertising from Google competitors, who seek to persuade users not to use Gmail because of its automated scanning features (like Microsoft's ubiquitous "Scroogled" campaign). Or anyone who uses another email service that utilizes automated scanning (like Plaintiffs Dunbar, Knowles, and Carrillo, who use Yahoo[14]) or is otherwise aware of industry scanning practices. (*Id.* ¶¶ 7, 19, 67.) Or advertisers who benefited from Google's automated scanning to deliver targeted ads.[15] Or anyone who learned about the automated processing in Gmail from family, friends, or colleagues who use Gmail, or even their school (Wong Decl. ¶¶ 85-100). Indeed, it is likely that these sorts of individuals collectively comprise the great majority of the proposed classes. To resolve their individual claims, a fact-finder would need to first identify these persons and then determine *when* they became aware of scanning, to identify which of their emails were sent with or without implied consent—an individualized inquiry many named Plaintiffs have recognized. (Somv. Decl. ¶¶ 26, 71, 86, 95.)

There is no conceivable way to resolve these inherently individualized issues on a classwide basis, which would require fact-intensive inquiries for each proposed class member and each email allegedly "intercepted" by Google. Certification, then, would strip Google of its due process right to defend itself, because the individual inquiries needed to do so would be impossible. *See Dukes*, 131 S. Ct. at 2561 ("a class cannot be certified on the premise that [a defendant] will not be entitled to litigate its statutory defenses to individual claims.").

b. Plaintiffs' efforts to avoid these individualized issues all fail.

Faced with this insurmountable obstacle to certification, Plaintiffs pose a series of arguments designed to obscure the relevant issues and avoid the "rigorous analysis" mandated under Rule 23. These arguments are unavailing.

First, Plaintiffs claim that Google's contractual terms are a "failed attempt at express"

[14] Yahoo scans emails specifically to show targeted ads. (*See* Somv. Decl., ¶ 116.)

[15] The Chin Declaration explains how Google advertisers specifically benefit from targeted ads in Gmail and yet are included within the proposed classes. (*See* Chin Decl., ¶¶ 78-81.)

consent and therefore Google cannot rely on the alternative defense of implied consent. (Mot. at 16.) But this ignores the black-letter law that consent can be based on *either* an express agreement *or* implied from circumstances. Google cannot be deprived of the implied consent defense simply because Plaintiffs dispute the meaning and application of Google's express terms.[16] Contrary to Plaintiffs' assertion, courts routinely examine evidence of express consent *and* implied consent in resolving wiretapping claims. *See, e.g.*, *Van Poyck*, 77 F.3d at 291-92 (resolving consent under ECPA based on evidence of a written agreement as well the inmate's knowledge of non-contractual disclosures); *Shefts*, 758 F. Supp. 2d at 631 (resolving consent based on an Employee Manual that applied to a employee along with non-contractual evidence showing he knew his emails and text messages could be monitored).

O'Donovan v. Cashcall, Inc., 278 F.R.D. 479 (N.D. Cal. 2011) is instructive. *O'Donovan* involved claims that a loan company initiated unauthorized electronic fund transfers ("EFTs"). As here, the plaintiffs claimed that consent could be resolved on a classwide basis by reviewing a uniform set of documents (the parties' loan agreements and transaction logs) to determine whether the defendant was authorized to make EFTs on certain dates. *Id*. at 494-95. The court rejected this argument, explaining that it could not limit its analysis to the contractual documents and was required to assess "any evidence CashCall may have that shows a specific borrower authorized or consented to [an] EFT" on a particular date. *Id*. Similarly here, even if Plaintiffs could show that Google's contractual terms do not authorize the automated scanning in Gmail, the parties would still have to resolve the separate issue of implied consent based on all of the non-contractual sources of information set forth above.[17]

---

[16] Plaintiffs' authorities on this issue are inapposite. In *Harris v. comScore, Inc.*, No. 11 C 5807, 2013 WL 1339262 (N.D. Ill. Apr. 2, 2013), the consent issues turned on the contractual terms of service because there were no additional disclosures explaining the data practices at issue and thus no basis for implied consent. *See id* at *1-3 (examining the various terms of service) and *6 ("[t]he scope of the plaintiffs' consent here is determined by that identical process, the ULA, and the Downloading Statement …."). Plaintiffs' other cases are even less relevant, as they simply note basic principles of contract interpretation and have nothing to do with the consent exception to a wiretapping claim. (*See* Mot. at 15-16.)

[17] Plaintiffs claim that Google's witness Aaron Rothman testified that the *only* materials relevant to assessing consent are contained in five specific documents. (Mot. at 15.) But Plaintiff's selective quotation and description of the witness's testimony ignore Mr. Rothman's clear explanation that he was simply listing the documents containing Google's *contractual* terms with

Second, Plaintiffs claim that (1) all of the evidence on consent will come from Google and (2) the Court can objectively determine if Google's disclosures are sufficient and apply those findings on a classwide basis. (Mot. at 15.) This is wrong on multiple levels. First, the assertion that Google is the lone source of disclosures is simply false, as demonstrated above. Indeed, it is curious that Plaintiffs would even make this claim because most learned about Google's alleged "interceptions" from *non*-Google sources—namely their own lawyers. (*See, e.g.*, Somv. Decl., ¶¶ 3, 17, 38, 49, 65.) Moreover, Plaintiffs concede that implied consent is based on a party's "*actual knowledge*," (Mot. at 22), which may differ from the self-serving interpretations that Plaintiffs seek to impose uniformly on every member of the class. For example, the current Complaint asserts that Google's post-March 2012 Privacy Policy "do[es] not address or obtain consent for" Google to use Gmail users' "email message content." (FAC ¶ 194.) But Plaintiff Dunbar testified to the contrary that the Privacy Policy allows Google to collect information on "how someone uses the Gmail service," including "the emails that they send and receive." (Somv. Decl., ¶ 24.) This discrepancy between Dunbar's "actual" understanding and Plaintiffs' proffered interpretation highlights the need to assess consent on an individualized basis.

Third, Plaintiffs argue that Google's disclosures "do not adequately disclose the *nature and use* of [Google's] interception." (Mot. at 20 (emphasis added).) But the relevant inquiry on consent is whether a communicating party is aware of the "interception" itself. *See* 18 U.S.C. § 2511(2)(d) (no liability where there is "consent" to the "interception"). Where a communicating party knows that a third-party will access the content of a communication, there is no additional requirement that the party must consent to the subsequent uses of that information.[18] This is apparent in Plaintiffs' own authorities, which focus on whether the claimant consented to the interception itself, *not* whether he was aware of all potential uses of the communication. *See Williams v. Poulos*, 11 F.3d 271, 281-82 (1st Cir. 1993) (finding no consent where employee was

---

Gmail users. (*See* Somv. Decl., ¶¶ 103-07.) Contrary to Plaintiffs' mischaracterization, Mr. Rothman went on to testify about numerous categories of *non-contractual* disclosures available from Google that describe the automated scanning in Gmail. (*Id.*)

[18] Under 18 U.S.C. § 2511(1)(c), a "use" claim exists only for the use of information "obtained through the interception … in violation of this subsection." Accordingly, where there is consent to the alleged "interception," there cannot be liability for any subsequent "use" of information.

aware of monitoring generally, without examining if employee knew the specific means of recording or the uses of the information). *See also United States v. Green*, 842 F. Supp. 68, 71 (W.D.N.Y. 1994) (implied consent applied where prison disclosed inmate calls would be recorded even though the inmates "were never told that … the prison could use the tapes as incriminating evidence in a criminal investigation …."). Nor does implied consent require an understanding of the technical methods by which the alleged "interception" occurs, so long as the party is aware that the content of a communication will be accessed. *See In re Pharmatrak, Inc.*, 329 F.3d 9, 20 (1st Cir. 2003) (collecting cases finding consent to the collection of website activity and finding "it would be unreasonable to infer that the clients had not consented merely because they might not understand precisely how the user demographics were collected").

Fourth, Plaintiffs claim that any consent is invalid because Google acted with the "purpose of committing [a] tortious act" under Section 2511(2)(d). (Mot. at 23.) This ignores the black letter law. The "criminal" or "tortious" purpose provision of Section 2511(2)(d) invalidates consent *only* where a defendant acts "with an *intent to injure* the other party …. For example, … for the purpose of blackmailing the other party, threatening him, or publicly embarrassing him." *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 515 (S.D.N.Y. 2001) (quotations omitted). This requires more than proving that the defendant committed a tort or even a crime—the plaintiff must prove that the *specific purpose* of the act was to cause harm. *Id.* at 518-19 (consent applied where plaintiffs did not allege "that [defendant's] 'primary motivation' or a 'determining factor' in its actions has been to injure plaintiffs tortiously"); *Boddie v. ABC*, 881 F.2d 267, 270 (6th Cir. 1989) ("[I]t is the *use* of the interception with intent to harm rather than the fact of interception that is critical to liability ....") (quotations omitted). Plaintiff does not offer any evidence (or even allege) that Google acted with the wrongful intent required under these standards. To the contrary, Plaintiff argues that Google acted with the *business motivation* to "avoid paying 'traffic acquisition costs'." (Mot. at 23.) This falls far short of the showing needed to invalidate consent.

Fifth, Plaintiff cites various TCPA cases for the proposition that "consent can be determined on a class-wide basis whenever 'individualized evidence' is not required." (Mot. at

20.) But these cases involved specialized sources of common proof available in the context of certain TCPA cases and have no application here.[19] If anything, these cases effectively confirm that certification is improper if such specialized evidence is unavailable, as is the case here.

In sum, certification should be denied because the individualized issues of implied consent are impossible to resolve on a classwide basis and will predominate over any common issues.

2. Plaintiffs Also Fail to Show That The Alleged "Interceptions" Can Be Identified on a Classwide Basis.

Under *Dukes*, a class action plaintiff must demonstrate that all class members suffered the "same injury" to satisfy commonality. 131 S. Ct. at 2550-51. Reflecting similar concerns, the Ninth Circuit has held that "'no class may be certified that contains members lacking Article III standing.'" *Mazza*, 666 F.3d at 594. Recently, the Supreme Court has emphasized that a plaintiff must establish "through evidentiary proof" that "damages are capable of measurement on a classwide basis." *Comcast*, 133 S. Ct. at 1432-33. Given these requirements for certification, Plaintiffs must demonstrate a viable classwide method to (1) identify the particular class members whose emails were allegedly "intercepted" (to establish standing and common injury), and (2) isolate the specific "intercepted" emails among the billions implicated by the proposed classes (to measure damages on a classwide basis).

Instead of addressing these critical issues, Plaintiffs sidestep them altogether by declaring that *all* emails are processed in a "uniform" manner. (*See, e.g.*, Mot. at 2 ("The uniform nature of Google's secret content extraction . . . make[s] this case perfectly suited for class treatment.").) This is demonstrably false.[20]

With respect to the [redacted], Plaintiffs ignore undisputed evidence that:

- [redacted] processing is *not* applied [redacted].

[19] *See Kavu, Inc. v. Omnipak Corp.*, 246 F.R.D. 642, 647 (W.D. Wash. 2007) (relying on the fact that phone numbers were obtained from a common commercial database); *Saf-T-Gard Int'l, Inc. v. Vanguard Energy Servs., LLC*, No. 12 C 3671, 2012 WL 6106714, at *5 (N.D. Ill. Dec. 6, 2012) (noting that the "key inquiry will be the manner in which VES developed its fax recipient list, not the nature of the relationship between VES and each putative plaintiff."); *Hinman v. M & M Rental Ctr., Inc.*, 545 F. Supp. 2d 802, 806 (N.D. Ill. 2008) (involving a common list compiled by a third party). *Compare* Note 11 above (collecting certification denials in TCPA cases.)

[20] Indeed, Plaintiffs and their counsel have access to massive body of discovery demonstrating that their blanket assertions of "uniform" scanning are meritless. (*See* Stewart Decl., ¶¶ 4-17.)

(Kapadia Decl., ¶ 28.)

- [redacted] processing was *not* applied to emails sent to Gmail or Google Apps users that were [redacted]. (*Id.* ¶ 18(a).)[21]
- [redacted] does *not* scan several kinds of [redacted]. (*Id.* ¶ 18(e).)
- [redacted] processing does *not* occur when the applicable servers are experiencing an outage, are undergoing regular maintenance, or return an error. (*Id.* ¶ 18(f-h).)
- Google Apps customers can configure their systems to entirely avoid COB processing, and can choose to do so for only some users and time periods. (Declaration of Brandon Long ("Long Decl."), at ¶ 3.)

Scanning by the [redacted] system also depends on various factors that will differ from person to person, and from email to email. For emails that Gmail and Google Apps users receive:

- [redacted] scanning applies only when the user [redacted]; if the user views an email on a mobile device or other methods in which ads are not shown, [redacted]. (Kapadia Decl., ¶ 10(b).)
- Similarly, if a Google Apps customer configures Google Apps not to display advertising, [redacted]. (*Id.* ¶ 10(c)(i).)
- As with [redacted] does not scan many types of [redacted]. (*Id.* ¶ 10(f).)
- As with [redacted] processing does not occur if the system is experiencing an outage, undergoing regular maintenance, or returns an error. (*Id.* ¶ 10(e).)

[redacted] scanning applies on an [redacted] for emails that Gmail/Google Apps users *send*. A user's sent emails are scanned by [redacted] only if the above conditions apply *and*:

- The email is an o[redacted];
- [redacted] to show ads in a specific section of the user's inbox;
- [redacted]; and
- [redacted]. (*Id.* ¶¶ 31-34.)

These are not merely hypothetical or trivial issues. For example, as many as [redacted] received in the Gmail system each week are flagged as spam, [redacted]

[21] [redacted], the sequence was changed so that [redacted] (Kapadia Decl., ¶ 18(a).) that Plaintiffs admit is legal.

[redacted]. (*Id.* ¶ 18(a).) And as much as [redacted] on Gmail involves a mobile device in which ads are not shown and [redacted] was not applied until only a few months ago. (*Id.* ¶ 10(c)(ii).)

Plaintiffs ignore these gaping exceptions to their claim of "uniform" processing and make no effort to explain how they can identify these categories of emails for which there is no colorable claim of "interception." By simply assuming (contrary to the record) that scanning is uniform and purporting to impose liability for *all* emails that were sent to, or received by, the putative class members, Plaintiffs' certification theory would award damages for a massive number of emails that were never "intercepted" under their own theories and deny Google the ability to defend the case. In many cases, this could result in windfall recoveries for class members whose emails were never "intercepted" at all. A class cannot be certified under these circumstances. *See, e.g.*, *In re Rail Freight Fuel Surcharge Antitrust Litig.*, 725 F.3d 244, 252-55 (D.C. Cir. 2013) (vacating class certification where the plaintiffs' proposed damages methodology was "prone to false positives"); *Mazur v. eBay Inc.*, 257 F.R.D. 563, 570 (N.D. Cal. 2009) (denying certification where plaintiffs alleged uniform wrongful conduct related to defendant's online auctions but had no method to identify the specific auctions in which class members were allegedly injured); *In re Flash Memory Antitrust Litig.*, No. C 07-0086 SBA, 2010 WL 2332081, at *12 (N.D. Cal. June 9, 2010) (denying certification where the proposed damages methodology "would … sweep in an unacceptable number of uninjured plaintiffs").

Plaintiffs suggest they will avoid these issues by using a claims process in which putative class members will submit information to identify the emails they believe are at issue.[22] But they have provided the Court no expert analysis or other evidence to conclude that a claims process will actually work. In fact, there is no claims process that could be applied here. Class members have no way to determine if any given email was processed by [redacted] and therefore cannot submit a claim to demonstrate an alleged "interception" (even setting aside the practical considerations of receiving and resolving claims information from potentially hundreds of

[22] Plaintiffs claim "[a] Class Member can easily provide a Message ID and related header information … that allows the Court and Google to 'ascertain whether an individual is a class member.'" (Mot. at 12-13.)

millions of class members). As explained in the Kapadia Declaration, email senders have no data in their own email accounts that could show if the emails they sent to Gmail or Google Apps users were scanned by [redacted] during the delivery process to the recipient. (Decl., ¶¶ 11, 20.) Nor would someone who received a message from a Gmail user have information to show whether that email was sent in a manner that might involve [redacted] scanning.[23] (*Id.* ¶ 11.)

Notably, Plaintiffs' vaguely defined claims process is the *only* method they propose for ascertaining the proposed class members and identifying the instances of alleged wrongful scanning. They do *not* propose any method based on accessing Google's internal data for the many millions of non-party Gmail users implicated by their claims—presumably because they recognize the massive practical hurdles of attempting any such analysis, as well as the legal bar to disclosure under the Stored Communications Act ("SCA"). Under the SCA, "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service . . . ." 18 U.S.C. § 2702(a)(1); *see also* 18 U.S.C. § 2702(b) (prohibiting disclosure of customer records). *See also Theofel v. Farey-Jones*, 359 F.3d 1066, 1074 (9th Cir. 2004) (compelling production of email messages in discovery would run afoul of "the specific [privacy] interests that the [SCA] seeks to protect") (quotations omitted). As Judge Grewal recognized in *Dunbar*, "[e]ven if Dunbar were only seeking production of the email communications in which he was the 'originator' (for which a voluntary exception could apply under 18 U.S.C. § 2702(b)(3)), Google may not be compelled to produce the emails and associated metadata that it maintains in electronic storage subject to the Stored Communications Act." (ECF No. 244 at 2.) These considerations bar Plaintiffs from relying on any classwide method based on accessing the emails of non-party Gmail users, even if they were to make (and the Court were to entertain) such a belated proposal in their reply brief.

In an effort to obscure these obstacles to certification, Plaintiffs repeatedly highlight the word "*endeavor*" throughout their Motion, apparently to suggest that a theory of "attempted"

[23] These difficulties apply even if class members opt to seek the minimum statutory damages under the wiretapping statutes. Even in this circumstance, Plaintiffs have not shown a viable method to show that all class members had even a single email "intercepted."

scanning somehow obviates the need to present a viable method to identify the emails that were *actually* scanned. (*See* Mot. at 1, 2, 4, 5, 7, 19, 20.) A claim for damages under ECPA or its state equivalents, however, "must be based on *actual interception, disclosure, or use* . . . . An endeavor . . . to do one of those things does not come within the scope of § 2520." *DirecTV, Inc. v. Hoverson*, 319 F. Supp. 2d 735, 737-38 (N.D. Tex. 2004) (emphasis added). *See also Thomas v. Thomas*, No. 1:11-CV-2336, 2012 WL 4895117, at *4 (M.D. Pa. Oct. 15, 2012) ("Plaintiff's position[] that [§ 2520(a)] require[s] only that the defendant endeavored or attempted to intercept a[] … communication … is incorrect."). Plaintiffs simply ignore this established law, which precludes the "endeavoring" claim that they allude to without citation.[24]

3. Individualized Issues Predominate The CIPA Claims.

Section 631 of CIPA, by its terms, applies only to communications that have a connection to California. Cal. Penal Code § 631 (prohibiting the interception of communications when they are "in transit or passing over any wire, line, or cable, or [are] being sent from, or received at *any place within this state*" (emphasis added)).[25] Here, the CIPA Class by definition consists of *non-*

[24] *See also DeVittorio v. Hall*, 347 F. App'x 650, 653 (2d Cir. 2009) (affirming dismissal of Section 2520 claim because plaintiffs failed "to adduce some evidence that their communications were, in fact, intercepted"); *DirecTV, Inc. v. Minor*, 420 F.3d 546, 549 (5th Cir. 2005) (requiring proof of "the key element of actual interception"); *Carpiniello v. Hall*, No. 07 Civ. 1956(PGG), 2010 WL 987022, at *5 (S.D.N.Y. Mar. 17, 2010) (ECPA's civil damages requires "an actual interception"); *DirecTV, Inc. v. Wallace*, 347 F. Supp. 2d 559, 565 (M.D. Tenn. 2004) ("an aggrieved person must have suffered an actual illegal interception, disclosure, or use of his or her communication before that person may initiate a civil suit under § 2520(a)."); *DirecTV, Inc. v. Cavanaugh*, 321 F. Supp. 2d 825, 831 (E.D. Mich. 2003) ("Together with § 2520, § 2511 provides for liability when [communications] are actually intercepted."); *DirecTV, Inc. v. DeCroce*, 332 F. Supp. 2d 715, 719 (D.N.J. 2004) (holding that the statutory language "demonstrates Congress's intent to limit civil liability under Section 2520(a) to the class of defendants who actually intercepted a communication"), *rev'd on other grounds by DirecTV, Inc. v. Pepe*, 431 F.3d 162 (3rd Cir. Dec. 15, 2005) ; *Minotty v. Baudo*, 42 So. 3d 824, 830 (Fla. Dist. Ct. App. 2010) (rejecting "assertion that an attempted interception would be actionable" under Florida wiretapping statute); Md. Code Ann. §§ 10-402, 10-410 (providing a cause of action only to persons whose communications are "intercepted, disclosed, or used" illegally).

[25] This limitation is consistent with the general presumption against extraterritorial application of California law. *See Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1207 (2011) ("we presume the Legislature did not intend a statute to be operative, with respect to occurrences outside the state"). Indeed, if CIPA were interpreted to cover interceptions with no connection to California, it would violate constitutional principles that bar a state from applying its law to conduct outside its borders. *See Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 814-22 (1985) (Kansas law could not be applied to the entire class where the majority of oil and gas deposits at issue were located outside of Kansas); *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 570-72 (1996) (state may not impose penalties "with the intent of changing the tortfeasors' lawful conduct in other States.").

California residents who generally did *not* send emails from California. And the alleged wrongful "devices" at issue are located *outside* California, meaning the alleged "interceptions" did *not* occur while emails were in transit through the state.[26] Each CIPA Class Member must therefore attempt to show that he or she sent emails to California residents that were "received at [a] place within [the] State." Cal. Penal Code § 631(a). Yet Plaintiffs propose no method to identify these isolated emails from the billions of emails sent by the CIPA Class, the great majority of which have no connection to California. Plaintiffs' own experiences confirm this. Plaintiff Brad Scott testified he has *never* sent emails to Gmail users in California, Plaintiff Harrington could only recall isolated emails with two people in California, and Plaintiff Kovler could not identify any emails he sent to California Gmail users. (Somv. Decl., ¶¶ 94, 42, 82.) The only way Google knows these critical facts is from deposing the CIPA Plaintiffs. There is no way to collect this sort of individual testimony from the millions in the CIPA Class, which poses another insurmountable obstacle certifying the CIPA claim.[27]

E. Choice Of Law Principles Also Preclude Certification of The CIPA Claims.

The CIPA claims also cannot be certified because choice of law principles preclude Plaintiffs from imposing California law on the other 49 states comprising a proposed CIPA Class.

1. California Does Not Have An Interest In Having Its Law Applied.

Under the California choice of law analysis, if "only one of the states has an interest in having its law applied," there is "no problem in choosing the applicable rule of law" as the law of the state having an interest in the dispute. *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 109 (2006) (quotation omitted). Here, the express purpose of CIPA is to protect *California residents*: "The Legislature by this chapter intends to protect the right of privacy of *the people of this state*." Cal. Penal Code § 630 (emphasis added). *See also Kearney*, 39 Cal. 4th at 119-20

[26] *See* Somv. Decl., ¶ 114, 115. Even if some emails transit over Google infrastructure in California those aspects of transmission do not involve the alleged "devices" or "interceptions." This limited transmission in California is therefore irrelevant under CIPA. (*See id.*) To the extent Plaintiffs contend that the mere transmission over non-intercepting equipment in California is sufficient under CIPA, they have not shown that this can be established on a classwide basis.

[27] Google does not have internal data that could be used to determine if the CIPA Class members corresponded with Gmail users who reside in California. (Kapadia Decl., ¶¶ 38-39.)

("there can be no question but that the principal purpose of [CIPA] is to protect the privacy of confidential communications of California residents *while they are in California*"); *Zephyr v. Saxon Mortg. Servs., Inc.*, 873 F. Supp. 2d 1223, 1231 (E.D. Cal. 2012) (finding that CIPA is intended "to protect California residents from having their conversations recorded by either instate or out-of-state callers without all parties' consent."). This express focus on California residents is consistent with choice of law principles that disfavor the application of a state's law to non-residents. *See Mazza*, 666 F.3d at 594 ("California's interest in applying its law to residents of foreign states is attenuated"); *Edgar v. MITE Corp.*, 457 U.S. 624, 644 (1982) ("While protecting local investors is plainly a legitimate state objective, the State has no legitimate interest in protecting nonresident shareholders.").

These authorities confirm California has no interest in applying CIPA to the claims of a class that consists *exclusively* of *non*-California residents, particularly where the alleged wrongful "devices" and "interceptions" are also outside of California and Plaintiffs have provided no basis to conclude that there is anything but a minimal connection to California recipients. This is dispositive of the choice of law analysis and precludes application of California law.

2. The Interests Of Others States Would Be Materially Impaired.

Even if the Court were to address the remaining aspects of the choice of law analysis, the same result would apply. The first step of the analysis asks whether the laws of the potentially affected states differ. (ECF No. 69 at 33.) Here, there are a host of significant differences between CIPA and the wiretapping statutes of the other 49 states. First, approximately 38 states preclude liability where a single party to the communication consents to the "interception," whereas CIPA requires the consent of all parties. *Kearney*, 39 Cal. 4th at 122 n.14. The Court previously questioned (without resolving) whether this difference is "material" for choice of law purposes and Plaintiffs have seized upon that statement to argue that these distinctions are irrelevant. (ECF No. 69 at 34:23-35:4; Mot. at 27.) Not only is the difference material, it could be *dispositive* in many cases. For example, if a fact finder concludes for a particular email that the non-Gmail user did not consent but the Gmail user *did* consent to automated scanning, that finding would preclude liability under the 38 state laws with a single-party consent exception; in

contrast, the non-Gmail user could still potentially pursue a claim if the minority rule under CIPA applies. This is a quintessential example of a material conflict. *Mazza*, 666 F.3d at 590 (a difference is material if it "make[s] a difference in th[e] litigation.").

There are a host of other materials conflicts as well. With respect to the 11 other states that, like California, have adopted a dual-party consent requirement:

- Some provide for different (in some cases greater) remedies than CIPA. For example, seven states allow recovery of punitive damages.[28] CIPA does not. Some states do not provide for injunctive relief.[29] CIPA does.[30]
- Pennsylvania law is limited to persons who send (as opposed to receive) emails, as the Court has held. (ECF. No. 69 at 43:8-13.) CIPA is not.
- Some states require plaintiffs to prove that they had either an objective or subjective expectation that their communications would remain "private."[31] Section 631 of CIPA does not.
- At least one dual-party consent state (and 12 single-party consent states) do not provide a private right of action for wiretapping at all.[32] CIPA does.
- At least one dual party consent state, along with several single-party consent states, exclude email from their wiretapping statutes.[33] Plaintiffs

[28] *See* Fl. Stat. § 934.10(c); Ill. Comp. Stat. Ann. § 5/14-6(1)(e); Md. Code Ann., Cts. & Jud. Proc. § 10-410(a)(2); Mass. Ann. Laws ch. 272, § 99(Q); Nev. Rev. Stat. Ann. § 200.690(1)(b)(2); N.H. Rev. Stat. Ann. § 570-A:11; 18 Pa. Const. Stat. § 5725. This is also true as to several single party consent states. *See, e.g.*, Haw. Rev. Stat. § 803-48 (Hawaii wiretap law provides for punitive damages); Minn. Stat. § 626A.13 (same, but as to Minnesota).

[29] *See* Mass. Ann. Laws ch. 272, § 99(Q); Md. Code Ann., Cts. & Jud. Proc. § 10-410; N.H. Rev. Stat. Ann. § 570-A:11.

[30] The Court previously noted that "differences in remedies alone are not dispositive" because any conflict could be resolved by "apply[ing] California law in a restrained manner." (ECF No. 304 35 n.11.) *Mazza*, however, held that differences in available remedies are "material" for choice of law purposes. *Mazza*, 666 F.3d at 591. Moreover, that reasoning does not apply where California provides for *lesser* remedies than the law of the other state.

[31] *See People v. Gariano*, 852 N.E.2d 344, 349 (Ill. App. Ct. 2006) (Illinois law); Mich. Comp. Laws Ann. § 750.539c (Michigan law); *Benford v. ABC*, 649 F. Supp. 9, 11 (D. Md. 1986) (Maryland law). This is also true as to certain single party consent states. *See, e.g.*, Conn. Gen. Stat. § 52-570d (a) (Connecticut law).

[32] Mont. Code Ann. § 45-8-213 (dual-party consent); single-party consent statutes with no private right of action include Ala. Code § 13A-11-31; Alaska Stat. § 42.20.310; Ark. Code Ann. § 5-60-120; Colo. Rev. Stat. § 18-9-303; Iowa Code § 727.8; Kan. Stat. Ann. § 21-4001; Ky. Rev. Stat. Ann. § 526.010; N.Y. Penal Law § 250.05; N.D. Cent. Code § 12.1-15-02; Okla. Stat. tit. 13 § 176; Or. Rev. Stat. § 165.543; S.D. Codified Laws § 23A-35A-20.

[33] *See Bailey v. Bailey*, 07-11672, 2008 WL 324156, at *8 (E.D. Mich. Feb. 6, 2008) (Michigan statute "was meant to prohibit eavesdropping in the traditional sense of recording or secretly listening to audible conversation"); *see also, e.g.*, Alaska Stat. §42.20.310 (applying to "oral conversations"); N.H. Rev. Stat. Ann. § 570-A:2 (applying to "telecommunication or oral

claim that CIPA does apply to emails.

By enacting these provisions that differ from CIPA, the various states have opted to define the scope of wiretapping liability in the manner that they believe best balances the protection of individual privacy while promoting business and other interests that might be affected by more expansive laws. As the Ninth Circuit emphasized, the choice of law analysis must recognize the "valid interest in shielding out-of-state businesses from what the state may consider to be excessive litigation" because "[i]n our federal system, states may permissibly differ on the extent to which they will tolerate a degree of lessened protection for consumers to create a more favorable business climate for the companies that the state seeks to attract to do business in the state." *Mazza*, 666 F.3d at 592-93.[34] *See Gianino v. Alacer Corp*. 846 F. Supp. 2d 1096, 1103 (C.D. Cal. 2012) (each state has a "compelling interest … in delineating the scope of recovery for the consumers under their own laws.").

As in *Mazza*, if California law were applied to the nationwide CIPA Class, the "foreign states would be impaired in their ability to calibrate liability to foster commerce" because they would be precluded from applying their own provisions that are designed to limit liability, as listed above. *Mazza*, 666 F.3d at 593. As just one example, several states have opted to preclude a private right of action for wiretapping altogether, reflecting the policy judgment that enforcement should be left to the discretion of the appropriate governmental bodies and not to civil litigation brought by private counsel. These policy choices and others should not be cast aside just because three non-California residents feel it would be more convenient to avoid their home states' laws and apply CIPA to a nationwide class.[35]

In contrast, the only purported California interest that Plaintiffs point to is the ability of California to regulate Google's business decisions in California. (Mot. at 26.) But CIPA, by its

---

communication").

[34] In enacting CAFA, Congress expressed concern that "many state courts faced with interstate class actions have undertaken to dictate the substantive laws of other states by applying their own laws to other states, resulting in a breach of federalism principles." S. Rep. No. 109-14, at 61 (2005), *reprinted in* 2005 U.S.C.C.A.N. 3, 57 (quotations and ellipses omitted).

[35] Plaintiffs acknowledge this by arguing that Maryland and Florida choice-of-law rules *require* the application of local law to the claims of Maryland and Florida residents, given the strong interests those states have in adjudicating the claims of their own residents. (Mot. at 25 n.12.)

express terms, is focused on protecting California residents and *not* regulating business decisions made in California, as discussed above. Even if this were part of the legislative purpose of CIPA (and there is no indication that it is), the Ninth Circuit has rejected similar arguments that California law should apply because the claims involve a California corporation and business policies formed in California:

> Plaintiffs contend that California [has an] interest[] . . . in regulating Honda, a California corporation. We recognize that California has an interest in regulating those who do business within its state boundaries . . . but we disagree . . . that applying California law to the claims of foreign residents concerning acts that took place in other states . . . is necessary to achieve that interest in this case.

Mazza, 666 F.3d at 594. *See also Schwartz v. Lights of Am.*, No. CV 11-1712-JVS(MLGx), 2012 WL 4497398, at *6 (C.D. Cal. Aug. 31, 2012) (rejecting claim that California law should apply to a nationwide class "because [defendant] is a California corporation that conducts its business exclusively in state.").[36]

For all these reasons, the Court should not certify the CIPA Class to impose CIPA as the uniform nationwide law of wiretapping.

F. Plaintiffs Are Inadequate Class Representatives With Atypical Claims.

In addition to the issues above, certification should be denied "if 'there is a danger that absent class members will suffer if their representative is preoccupied with defenses unique to it.'" *Hanon v. Dataproducts Corp.*, 976 F.2d 497, 508 (9th Cir. 1992).

Here, despite claiming that automated scanning "shocked" them (Kolb and J.K.), "made [his] heart sink" (Scott), and affected private matters "near and dear to his heart" (Kovler), no Plaintiff took any meaningful action to avoid Gmail. Instead, all Plaintiffs continued to use their Gmail or Google Apps accounts (in the case of the Gmail Plaintiffs) or to communicate with Gmail users (in the case of the Non-Gmail Plaintiffs) even *after* filing lawsuits confirming their

[36] The CIPA Plaintiffs point out that Google's TOS contains a California choice of law provision. (Mot. at 29:7-13.) But the fact that California law applies to non-California residents who have agreed to Google's terms is irrelevant to determining the law that should apply to CIPA Class members who are not bound to the TOS and cannot avail themselves of its choice of law and venue provision. In fact, the CIPA Plaintiffs emphasize that "Plaintiffs and Class Members are non-Gmail subscribers" and do not allege any connection to Google's TOS. (FAC ¶ 392.)

knowledge of automated scanning. (Somv. Decl., ¶¶ 5, 18, 34, 39, 52, 67, 81, 89, 98.) These include emails with family members, church parishioners, and clients to whom some Plaintiffs owe a fiduciary duty. (*See id.* ¶¶ 5, 37, 39) Yet Plaintiffs never notified these individuals that their emails were being allegedly "intercepted" by Google's automated scanning—calling into question whether they actually view Google's conduct to be improper at all. (*Id.* ¶¶ 41, 53, 67, 89.) Worse, most Plaintiffs contend that statutory damages apply to *all* of their emails involving Gmail, even *after* they became aware of Google's practices. (*Id.* ¶¶ 20, 35, 40, 69.) These circumstances give rise to a specialized defense that Plaintiffs not only consented to the alleged "interceptions" but intentionally sent emails to artificially increase their statutory recovery. *See Shields v. Smith*, No. C-90-0349 FMS, 1991 WL 319032, at *4 & n.3 (N.D. Cal. Nov. 4, 1991) (plaintiff deemed inadequate where his stock purchase appeared to have been made "to pursue a lawsuit" and "this activity is likely to become the focus of the litigation to the detriment of other class members").[37]

There are also a host of other specialized issues that will preoccupy the Plaintiffs in litigating their individual claims but do not broadly apply to class members. For example, Plaintiff Fread waged a year-long campaign to stop the migration of his email account to Google Apps, including providing testimony before the State legislature and engaging in correspondence with the FTC and the Department of Education in which he exhibited detailed knowledge of the scanning in Gmail. He ultimately agreed to use his Google Apps account but signed a "Statement of Agreement under Duress" to purportedly preserve his objections. The consent issues for Fread's case will turn on these highly unusual facts regarding his purported duress, which seem to have nothing to do with the claims of other class members.[38] (Somv. Decl. ¶¶ 28-33.)

[37] Indeed, Plaintiffs may not even have standing to pursue their individual claims at all, let alone to represent the interests of the proposed class. *See Meaunrit v. Pinnacle Foods Grp., LLC*, No. C 09–04555 CW, 2010 WL 1838715, at *3 (N.D. Cal. May 5, 2010) ("[Plaintiffs] cannot create an injury by taking unilateral action unhinged from Defendant's conduct.").

[38] Other examples of unique issues include (1) Plaintiff Carrillo's and J.K.'s use of Gmail accounts that they share with others, which introduces novel questions of whether they can unilaterally seek recovery for their joint emails, (*Id.* ¶¶ 6, 53.), (2) some of the Non-Gmail Plaintiffs also have Gmail accounts, which raises specialized issues of consent and also calls into question their ability to apply independent judgment on behalf of the Non-Gmail Classes, (*See e.g., id.* ¶¶ 64), and (3) Plaintiff Brent Scott works for a company that has represented Google in

A proposed class representative is also inadequate where he or she lacks the ability or willingness to "serve the necessary role of 'check[ing] the otherwise unfettered discretion of counsel in prosecuting the suit.'" *Welling v. Alexy*, 155 F.R.D. 654, 659 (N.D. Cal. 1994) (plaintiff deemed inadequate where, among other things, he "expressed an intention not to supervise the amount of time spent by his attorneys in prosecuting the case."); *Burkhalter Travel Agency v. MacFarms Int'l, Inc.*, 141 F.R.D. 144, 153-54 (N.D. Cal. 1991) (plaintiff deemed inadequate due to his "'alarming unfamiliarity'" with the case where he did not understand basic aspects of the case including the definitions of the proposed class).

Even in the lawyer-driven world of class actions, the Plaintiffs' testimony here showed an lack of knowledge about the litigation that was startling in many circumstances. For instance, Plaintiff Harrington did not know if scanning for targeted ads is part of this litigation, even though it is the central allegation in the complaints he lent his name to. (Somv. Decl., ¶ 43.) Several Plaintiffs also stated personal positions that conflict with those taken by their lawyers, reflecting a failure to check the "unfettered discretion" of counsel. For example, J.K. acknowledged he has no issue with automated scanning to automatically organize emails by subject matter for a user's convenience, yet his Complaint alleges that the very process that implements this feature is an illegal intercepting "device." (*Id.* ¶ 57.) Similarly, Angela Kolb testified she has no objection to the scanning of emails to identify dates so that users can create calendar entries, but acknowledged the Complaint nonetheless targets such scanning. (*Id.* ¶ 58.) In fact, some Plaintiffs openly disavowed any oversight of their attorneys. For example, Plaintiff Kovler (himself an attorney) said he "cannot imagine challenging [his lawyers'] expertise." (*Id.* at ¶ 83.) These admissions disqualify Plaintiffs from acting as class representatives. *Azoiani v. Love's Travel Stops & Country Stores, Inc.*, No. EDCV 07-90 ODW, 2007 WL 4811627, at *2 (C.D. Cal. Dec. 18, 2007) (plaintiff deemed inadequate where his testimony showed that "not only has he ceded all control to his counsel, but he had very little knowledge of the case to begin with.").

---

multi-billion dollar transactions and acknowledged he was unsure if his employment would affect his ability to pursue this case (*Id.* ¶¶ 102).

G. The Proposed Class Also Fails The Superiority Requirement of Rule 23(b)(3).

Certification is routinely denied where the claims at issue provide sufficient incentives for individual claims. For example, in *Antoninetti v. Chipotle Mexican Grill, Inc.*, No. 06cv02671 BTM (WMc), 2012 WL 3762440, at *7 (S.D. Cal. Aug. 28, 2012) the court denied certification on for lack of superiority where the claims at issue provided for damages "in the amount of $4,000 for each particular occasion" and "attorneys' fees and costs." *See also Rowden v. Pac. Parking Sys., Inc.*, 282 F.R.D. 581, 586-87 (C.D. Cal. 2012) (denying certification where claim permitted statutory damages "between $100 and $1000," as well as attorney's fees, costs, and punitive damages). The available remedies here are equivalent or greater, providing for (1) damages in the amount of $100 per day of violation or $10,000, whichever is greater[39]; (2) attorney's fees and costs; and (3) punitive damages. *See* 18 U.S.C. § 2520. As in *Rowden* and *Antoninetti*, the statutes at issue provide claimants and plaintiffs' counsel with significant monetary incentives to pursue individual claims.[40] Under these circumstances, a class action is not a "superior" method of resolving the claims at issue.

IV. CONCLUSION

For the foregoing reasons, Google respectfully request that class certification be denied as to all claims and all proposed classes.

[39] Because these statutory damages are designed to facilitate *individual* claims, it would raise serious due process concerns to apply them in the context of a class action that threatens Google with the risk of a massive damages award that bears no relation to any harm actually sustained by any class member. *See Maracich v. Spears*, 133 S. Ct. 2191, 2209 (2013) (noting, but not deciding, the question of "whether principles of due process and other doctrines that protect against excessive awards would come into play" in the context of a class action involving a claim with statutory damages); *Fraley v. Facebook, Inc.*, No. CV-11-01726 RS, 2013 WL 4516819, at *4 (N.D. Cal. Aug. 26, 2013) (explaining, in the context of class claims involving statutory damages of $750 per person that "[g]iven the class size, it is not plausible that class members could recover the full amount of the statutory penalties in any event, as such a judgment would pose due process concerns and threaten Facebook's existence.").

[40] The Court need look no further than the statements of Plaintiffs' own counsel, who repeatedly confirmed they intend to proceed with Plaintiff Dunbar's claims on an individual basis regardless of whether any class is certified. (*See* Somv. Decl., ¶ 117.)

Dated: November 21, 2013

COOLEY LLP
MICHAEL G. RHODES (116127)
WHITTY SOMVICHIAN (194463)
KYLE C. WONG (224021)

/s/ Whitty Somvichian

Attorneys for Defendant GOOGLE INC.

1341555/SF