COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT
NO. SJC-12103

DEBRA L. MARQUIS
Plaintiff/Appellant

v.

GOOGLE, INC.
Defendant/Appellee

ON APPEAL FROM A JUDGMENT OF THE SUFFOLK SUPERIOR COURT

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PLAINTFF/APPELLANT

Marc Rotenberg
BBO# 55048
Caitriona Fitzgerald
BBO# 673324
Alan Butler
Electronic Privacy
Information Center
(EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

October 24, 2016

CORPORATE DISCLOSURE STATEMENT

Pursuant to S.J.C. Rule 1:21 *amicus curiae* Electronic Privacy Information Center ("EPIC") states that it is a District of Columbia corporation with no parent corporation or publicly-held company with a 10 percent or greater ownership interest. EPIC is a non-profit, non-partisan corporation, organized under section 501(c)(3) of the Internal Revenue Code.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF THE *AMICUS CURIAE*[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. The EPIC State Policy Project is based in Somerville, Massachusetts. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other democratic values. The EPIC Advisory Board includes renowned legal scholars and technology experts. EPIC maintains one of the top privacy sites in the world, epic.org.

EPIC has participated as amici in cases before the Supreme Judicial Court, as well as other courts. *See*, *e.g.*, *Commonwealth v. White,* 475 Mass. 583 (2016) (search and seizure of a cell phone); *Commonwealth v. Connolly,* 454 Mass. 808 (2009) (use of a GPS tracking device); *Nelson v. Salem State College,* 446 Mass. 525 (2005) (employee privacy in the state workplace); *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (whether email can be "intercepted" in violation of federal wiretap law while it is temporarily stored on an email server); *Jennings v. Broome*, 401 S.C. 1

[1] EPIC Appellate Advocacy Fellow John Davisson assisted in the preparation of this brief.

(2012), cert. denied, 133 S. Ct. 1806 (2013) (concerning the scope of protections for stored e-mail under the Electronic Communications Privacy Act); *Ben Joffe v. Google,* 746 F.3d 920 (2013) (Google's civil liability under the Wiretap Act for interception of Wi-Fi payload data); *Bunnell v. Motion Picture Assoc. of America*, 567 F.Supp.2d 1148 (2008) (whether the Wiretap Act protects e-mail messages in circumstances when the messages are briefly stored while they pass through mail servers).

SUMMARY OF THE ARGUMENT

At issue in this case is the systematic data mining of millions of private email messages each day. Google intercepts these private communications and stores, examines, and classifies their contents in order to generate advertising revenue. The plaintiff in this case represents non-Gmail users who, through no fault of their own, have had their private messages intercepted and analyzed by Google for the company's own commercial benefit.

Google's scanning of private email is far more intrusive than the interception of private communications already prohibited by Massachusetts law. Not only does Google examine keywords in private

communications to profile users and generate advertising revenue, Google also links the user's Google search queries and clicks, the user's Google Profile, and other Google account information that is available to Google. Even if Gmail subscribers were to accept such business practices (and amici does not concede they do), it is impracticable for non-Gmail subscribers, who receive no formal notification of this practice, to consent to such interception and invasive profiling. It is also not possible for users to be aware of the scope and nature of email analysis when the company has routinely and secretly modified its data collection and profiling practices over the last 15 years.

The lower court erred when it denied class certification in this case. General knowledge of Google's business practices is not akin to consent, especially for non-Gmail users who have no contractual relationship with Google. Even if Google had publicly disclosed its business practices, the Commonwealth could not have intended for a mere disclosure to eliminate privacy protections under the Wiretap Act. Such a view would eviscerate Wiretap Act protections for Internet users as well as users of telephone

service. It would permit the interception of private communications without any indication of express or implied consent from the users.

ARGUMENT

I. Google's email data mining is even more invasive than the interception prohibited by the Commonwealth's Wiretap Act.

Since its inception, Google has collected more personal data and mined the contents of more private communications than any other company. Gmail was specifically designed to mine personal communications data and generate advertising revenue for Google. *See* Gould, *The Natural History of Gmail Data Mining*, Medium (June 24, 2014).[2] Since Gmail was released in 2004, Google has continually expanded the scope of its data collection by integrating personal information from search, video viewing, maps, and other services. Google, How Gmail Ads Work (2016).[3] Google also manages email accounts for businesses, educational organizations, and internet service providers (which do not use an @gmail.com address), a program known as "Google Apps" or "G Suite". Memorandum of Decision and

[2] https://medium.com/@jeffgould/the-natural-history-of-gmail-data-mining-be115d196b10#.xsrzusxzj.
[3] https://support.google.com/mail/answer/6603

Order on Plaintiff's Motion for Class Certification, *Marquis v. Google*, No. SUCV2011-02808-BLS1 at 3 (MA June 19, 2014) ("C.C. Dec."). Recipients of email from organizations that use Google Apps may not even know that their email is subject to scanning by Google as the email domain will not be "gmail.com". Miller, Google: Let Us Opt Out of Your Data Mining Machine, Wired (Oct. 2010).[4]

Prior to the launch of Gmail, Google developed methods to mine both "internal" and "external" email data, including the contents of the subject line, the to/from information, the topics discussed in the message, the topics relevant to linked attachments and embedded hyperlinks, geographic information about the sending and receiving parties, and other profile information. See How Gmail Ads Work, *supra*. See also U.S. Patent Application No. US 10/452,830 (filed June 2, 2003)[5]; EPIC, *Gmail Privacy FAQ*.[6] Prior to 2010, the message data was not extracted until after a user opened the email. Transcript of Proceedings Before the Honorable Lucy H. Koh at 39, *In re Google Inc. Gmail*

[4] https://www.wired.com/insights/2012/10/google-opt-out/.
[5] https://www.google.com/patents/US20040059712.
[6] https://epic.org/privacy/gmail/faq.html.

Litigation, No. 13-MD-02430, 2014 WL 1102660 (N.D. Cal. Feb. 27, 2014).[7] Then, beginning in 2010, Google concluded that it was missing out on a lot of user data when individuals were not opening their emails, were opening them on mobile devices, or were "Google Apps" users who were not served ads. *Id.* In order to increase the amount of personal data it collected, Google began using its "Content Onebox" (COB) system to scan messages during the delivery process, mining data even if the user never opened the email. *Id.* at 39-40; Rosenblatt, Google Wants E-mail Scanning Information Blocked, Bloomberg Technology (Mar. 14, 2014).[8]

The inner workings of the COB system are "shrouded in mystery" and Google has sought to exclude them from the public record in this and other Gmail-related suits. But based on what has been publicly disclosed, the COB uses "machine learning" algorithms to discern the "actual meaning of email messages." Gould, Courts Docs Show How Google Slices Users Into

[7] http://www.privacysurgeon.org/blog/wp-content/uploads/2014/08/Transcript-of-2.27.14-Proceedings-1.pdf.
[8] https://www.bloomberg.com/news/articles/2014-03-14/google-wants-e-mail-scanning-information-blocked.

'Millions of Buckets', Medium (Apr. 30, 2015).[9] This is a significant expansion from the prior "keyword" based scanning, and the data collected enables Google to build the most extensive user profiles in the world. Google has made every effort to thwart public and media access to understanding of these business practices. Davis, News Orgs Oppose Attempt To Seal Records In Gmail Privacy Case, MediaPost (Feb. 24, 2014).[10] (The news organizations seeking access to more information about Google' email scanning techniques include Atlantic Media, Forbes LLC, National Public Radio, Inc., The New York Times Company, and Politico, among others.)

Google's effort to exclude the history of the 2010 transition to COB from the public record was denied in the Northern District of California. Simon Davies, US Court Rejects Google's Attempt to Seal Transcript and Documents, The Privacy Surgeon (2014).

Google uses data from private communications to generate revenue by selling targeted advertisements

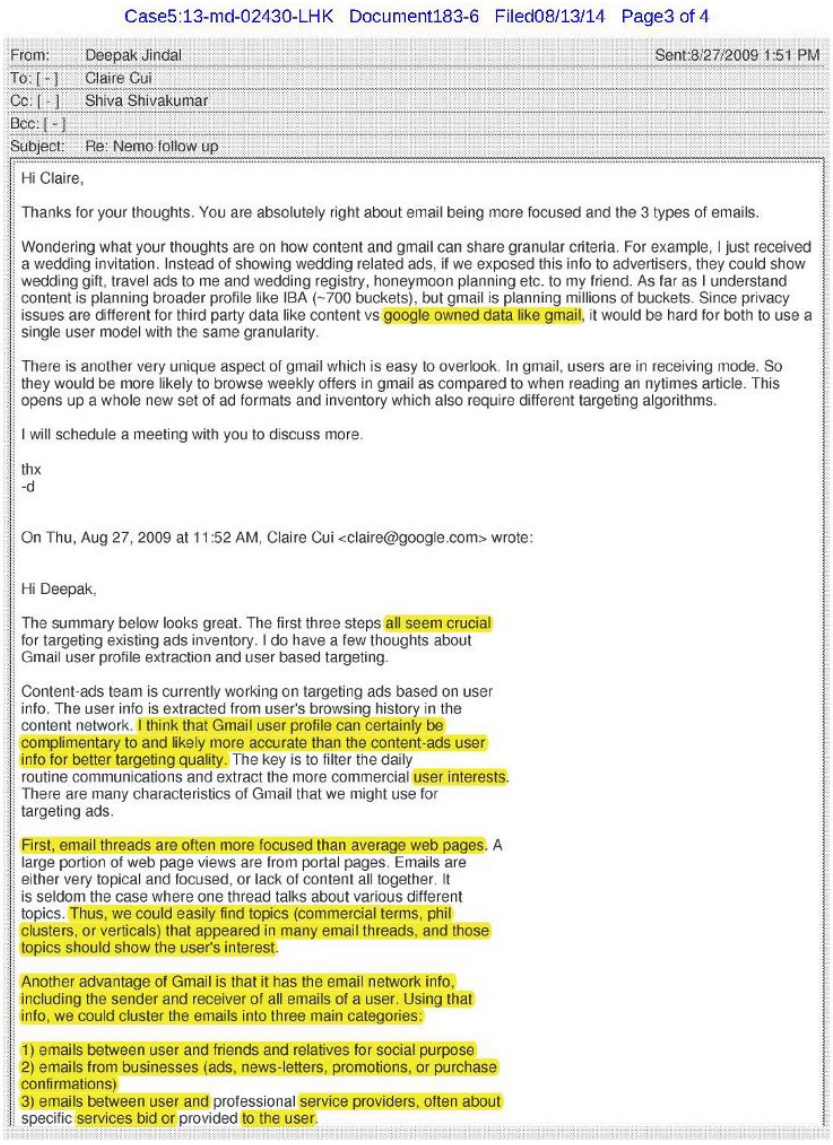
[9] https://medium.com/@jeffgould/courts-docs-show-how-google-slices-users-into-millions-of-buckets-ec9c768b6ae9#.ij5ewmm54.
[10] http://www.mediapost.com/publications/article/220151/news-orgs-oppose-attempt-to-seal-records-in-gmail.html

based on certain keywords. Defendant Google Inc's Motion to Dismiss at 3, *In re Google Inc. Gmail Litigation*, No. 13-MD-02430, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014). The Gmail data mining system "operates by identifying words in an email that may be relevant for advertising purposes," and subsequently uses the words in these private messages "to match an advertisement" and "show [it] to the Gmail user when he or she views the email." C.C. Dec. at 13. Gmail uses "content extraction" (the term used in Google's patents) on incoming and outgoing email in order to target advertising to Gmail users. U.S. Patent Application No. US 10/452,830 (filed June 2, 2003).[11] For example, if the user is having a private email conversation about applying for a job, Gmail will scan those messages and use the mined data to target advertising related to that topic. *Id.* at 0044.

Google also compiles this and other data to build intricate profiles of individuals based on their private browsing and communications habits. For example, Google looks at all the purchase confirmations in the user's inbox to build a profile

[11] https://www.google.com/patents/US20040059712.

of what the user may buy next. See Gould, *"millions of buckets"*, *supra*. The publication of internal Google emails recently revealed that Gmail "can sort users not just into a few thousand demographic and interest categories, but into literally millions of distinct 'buckets'":



Case5:13-md-02430-LHK Document183-6 Filed08/13/14 Page3 of 4

From: Deepak Jindal Sent:8/27/2009 1:51 PM
To: [-] Claire Cui
Cc: [-] Shiva Shivakumar
Bcc: [-]
Subject: Re: Nemo follow up

Hi Claire,

Thanks for your thoughts. You are absolutely right about email being more focused and the 3 types of emails.

Wondering what your thoughts are on how content and gmail can share granular criteria. For example, I just received a wedding invitation. Instead of showing wedding related ads, if we exposed this info to advertisers, they could show wedding gift, travel ads to me and wedding registry, honeymoon planning etc. to my friend. As far as I understand content is planning broader profile like IBA (~700 buckets), but gmail is planning millions of buckets. Since privacy issues are different for third party data like content vs google owned data like gmail, it would be hard for both to use a single user model with the same granularity.

There is another very unique aspect of gmail which is easy to overlook. In gmail, users are in receiving mode. So they would be more likely to browse weekly offers in gmail as compared to when reading an nytimes article. This opens up a whole new set of ad formats and inventory which also require different targeting algorithms.

I will schedule a meeting with you to discuss more.

thx
-d

On Thu, Aug 27, 2009 at 11:52 AM, Claire Cui <claire@google.com> wrote:

Hi Deepak,

The summary below looks great. The first three steps all seem crucial for targeting existing ads inventory. I do have a few thoughts about Gmail user profile extraction and user based targeting.

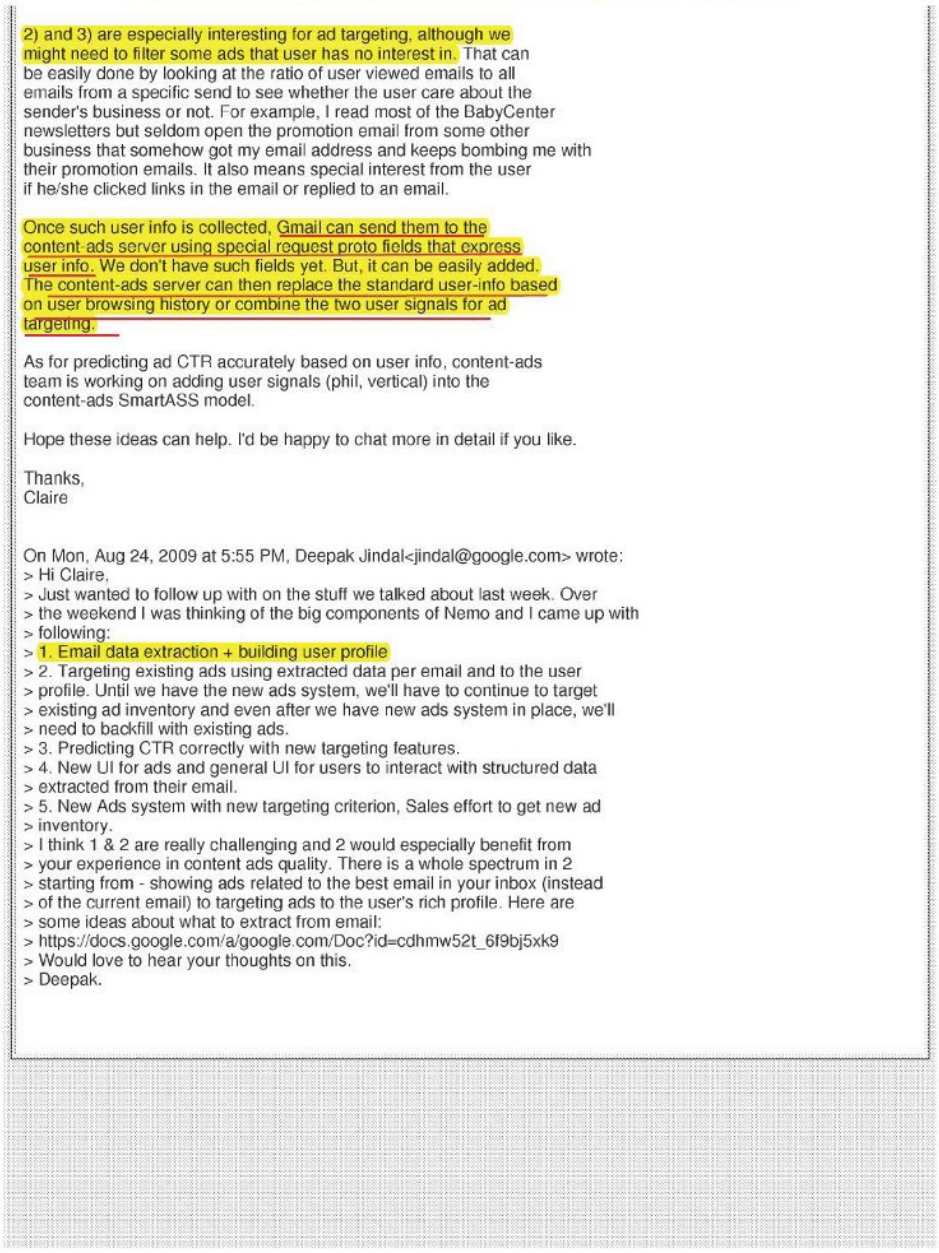
Content-ads team is currently working on targeting ads based on user info. The user info is extracted from user's browsing history in the content network. I think that Gmail user profile can certainly be complimentary to and likely more accurate than the content-ads user info for better targeting quality. The key is to filter the daily routine communications and extract the more commercial user interests. There are many characteristics of Gmail that we might use for targeting ads.

First, email threads are often more focused than average web pages. A large portion of web page views are from portal pages. Emails are either very topical and focused, or lack of content all together. It is seldom the case where one thread talks about various different topics. Thus, we could easily find topics (commercial terms, phil clusters, or verticals) that appeared in many email threads, and those topics should show the user's interest.

Another advantage of Gmail is that it has the email network info, including the sender and receiver of all emails of a user. Using that info, we could cluster the emails into three main categories:

1) emails between user and friends and relatives for social purpose
2) emails from businesses (ads, news-letters, promotions, or purchase confirmations)
3) emails between user and professional service providers, often about specific services bid or provided to the user.

CONFIDENTIAL - ATTORNEYS' EYES ONLY GOOG000733356



2) and 3) are especially interesting for ad targeting, although we might need to filter some ads that user has no interest in. That can be easily done by looking at the ratio of user viewed emails to all emails from a specific send to see whether the user care about the sender's business or not. For example, I read most of the BabyCenter newsletters but seldom open the promotion email from some other business that somehow got my email address and keeps bombing me with their promotion emails. It also means special interest from the user if he/she clicked links in the email or replied to an email.

Once such user info is collected, Gmail can send them to the content-ads server using special request proto fields that express user info. We don't have such fields yet. But, it can be easily added. The content-ads server can then replace the standard user-info based on user browsing history or combine the two user signals for ad targeting.

As for predicting ad CTR accurately based on user info, content-ads team is working on adding user signals (phil, vertical) into the content-ads SmartASS model.

Hope these ideas can help. I'd be happy to chat more in detail if you like.

Thanks,
Claire

On Mon, Aug 24, 2009 at 5:55 PM, Deepak Jindal<jindal@google.com> wrote:
> Hi Claire,
> Just wanted to follow up with on the stuff we talked about last week. Over
> the weekend I was thinking of the big components of Nemo and I came up with
> following:
> 1. Email data extraction + building user profile
> 2. Targeting existing ads using extracted data per email and to the user
> profile. Until we have the new ads system, we'll have to continue to target
> existing ad inventory and even after we have new ads system in place, we'll
> need to backfill with existing ads.
> 3. Predicting CTR correctly with new targeting features.
> 4. New UI for ads and general UI for users to interact with structured data
> extracted from their email.
> 5. New Ads system with new targeting criterion, Sales effort to get new ad
> inventory.
> I think 1 & 2 are really challenging and 2 would especially benefit from
> your experience in content ads quality. There is a whole spectrum in 2
> starting from - showing ads related to the best email in your inbox (instead
> of the current email) to targeting ads to the user's rich profile. Here are
> some ideas about what to extract from email:
> https://docs.google.com/a/google.com/Doc?id=cdhmw52t_6f9bj5xk9
> Would love to hear your thoughts on this.
> Deepak.

CONFIDENTIAL - ATTORNEYS' EYES ONLY GOOG000733357

Id.

Google's email scanning practices are in constant flux. Until recently, Google did not connect a user advertising profile with an actual identity. However,

Google recently changed its business practices. The company now combines an individual's internet browsing habits with the personal information Google knows about the individual, including their name. Angwin, Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking, ProPublica (Oct. 21, 2016).[12] "The practical result of the change is that the DoubleClick ads that follow people around on the web may now be customized to them based on your name and other information Google knows about you. It also means that Google could now, if it wished to, build a complete portrait of a user by name, based on everything they write in email, every website they visit and the searches they conduct." *Id.*

The change in business practices provides further evidence that Internet users could not reasonably have "actual knowledge" of the scope of the company's data mining practices. Regarding Google's decision to link user identity to advertising profiles, almost ten years have passed since the potential problem was first identified. When Google first acquired

[12] https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking

DoubleClick, the leading provider of Internet-based advertising, in 2007, EPIC and other leading consumer protection organizations filed a complaint with the Federal Trade Commission (FTC), urging the Commission to assesses the ability of Google to record, analyze, track, and profile the activities of Internet users with data that is both personally identifiable and data that is not personally identifiable. See EPIC, Privacy? Proposed Google/DoubleClick Merger.[13] The FTC failed to act and now Google is implementing exactly the practices EPIC warned of in its complaint. But for typical Internet users, who do not continuously monitor the company's constantly changing email practices, the recent change is correctly described by ProPublica: "Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking." Angwin, *supra.*

The Massachusetts Wiretap Act was adopted to prohibit the interception of private communications except in strictly limited circumstances such as pursuant to a court order or with the permission of both parties. G.L. c. 272, § 99. The law was amended in 1968 to prohibit unauthorized interceptions by

[13] https://epic.org/privacy/ftc/google/.

service providers and other non-governmental entities. *Id.*, as amended through St. 1968, c. 738. The potential for service provider eavesdropping was one of the primary concerns that drove the legislature to amend the law. *Commonwealth v. Ennis*, 439 Mass. 64, 69 (2003). In fact, the 1968 amendments to the Wiretap Act were prompted by news of a phone company's monitoring that had been made public in a 1966 *Boston Herald* article. Interim Report of the Special Commission on Electronic Eavesdropping, 1967 Senate Doc. No. 1198, at 4. In response to this revelation, the Special Commission recommended that the Legislature adopt new provisions "to insure that the privacy of the subscribers' telephone conversations [would] be protected." The Report of the Special Commission on Electronic Eavesdropping, 1968 Senate Doc. No. 1132, at 7. The preamble to the Wiretap Act states, in relevant part:

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

G.L. c. 272, § 99(A).

It is simply absurd to suggest that the legislature expected the prohibition on wiretapping to be inapplicable in cases where a communications service provider announced in general terms that they would begin monitoring calls. Yet, despite the clear statutory prohibition on the interception of private communications, the lower court in this case found that whether individual class members "knew about" Google's email data mining program based on a so-called "panoply of sources" discussed in *In re Google Inc. Gmail Litigation*, No. 13-MD-02430, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014), was a dispositive and individualized factual question that precluded class certification under Rule 23(b). C.C. Dec. at 21, 26.

The lower court's decision flips this important privacy law entirely on its head and would completely eliminate the two-party consent requirement. Rather than finding that a defendant must prove that their otherwise unlawful interception of a private communication was done pursuant to a limited exception or when "given prior authority by all parties to [the] communication," G.L. c. 272, § 99(B)(4), the lower court found that the plaintiffs must prove that the

interception was in fact "secret." C.C. Dec. at 23–24. But mere knowledge of the possibility that a communication could be intercepted is not sufficient to establish consent to the collection of private communications. See *Williams v. Poulos*, 11 F.3d 271, 281 (1st Cir. 1993) (finding that even where a CEO had been informed that his company had a system for monitoring calls, he did not impliedly consent to such monitoring).

There is no evidence in the record that non-Gmail users have consented to monitoring by Google for advertising purposes. In fact, Google has argued throughout this case and in other related cases that individuals, and non-Gmail users in particular, are not provided any notification that their messages are subject to interception, C.C. Dec. at 16, and further that it would be impossible for an individual to know whether any particular email would be processed as Google concedes that it mines some, but not all, communications data. C.C. Dec. at 12. ("Google's processing of email is not uniform, and the text of an email may or may not be scanned based on factors that differ from user to user and from message to message.

. . . [M]any emails are rejected and never delivered or scanned.").

Yet, despite these well-established facts, the lower court concluded that individual factual inquiries predominate the claims in this case. That conclusion is based on the faulty premise that a class member's awareness of general public disclosures and news stories about Google's email data mining could be sufficient to imply that they had consented to interception.

Google is asking this Court to accept that members (who are not Gmail subscribers) have actual knowledge of the extent of interception, scanning, profiling, and analysis of their private communications by the company when they send an email to a user of a Google service, who may or may not be identified with the gmail.com. It would undermine the purpose of the Wiretap Act to infer that an individual's general awareness that an email service provider might intercept private communications could constitute implied consent to interception and "actual knowledge" of such interception. If the same rule were applied to telephone communications, knowledge that a telephone company could tap an individual's phone at

any time would mean the individual had "actual knowledge" that her phone calls were being intercepted, and impliedly consented to such interception. The Wiretap Act would not permit a telephone company to use automated systems to record phone conversations, and it should not permit an email provider to do so either.

II. Informed consent is a pillar of electronic privacy law and an indispensable part of the Massachusetts Wiretap Act

In prohibiting persons from "secretly hear[ing]" or "secretly record[ing]" communications without "authority by all parties," G.L. c. 272, § 99(B)(4), the Massachusetts Wiretap Act reinforces a bedrock principle of privacy law: private communications data should not be collected, used, or disseminated without informed consent. Massachusetts state legislators realized that the harms they sought to prevent in the Wiretap Act–eavesdropping on and use of private communications–would persist unless they prohibited all interception conducted without "prior authority by all parties." G.L. c. 272, § 99(B)(4).

In the digital context, it is impossible to infer that an individual has consented to monitoring based on vague indications of how and when one's personal

data might be processed. Rather, an individual must be presented with clear and particularized information. Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 Harv. J.L. & Tech. 229, 246 (2004) ("Informed consent requires not only that data processors provide the relevant information, but also that individuals are aware of the mode and the extent of data processing to which they are consenting."); Julie Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 Stan. L. Rev. 1373, 1396 (2000) ("Freedom of choice in markets requires accurate information about choices and their consequences[.]").

The importance of informed consent is reflected in a wide range of communications privacy laws. See, *e.g.*, Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227(b)(1)(A) ("It shall be unlawful . . . to make any call (other than a call . . . made with the prior express consent of the called party) using any automatic telephone dialing system[.]"); Wiretap Act, 18 U.S.C. § 2511(2)(c) (prohibiting the interception of communications "without prior consent to such interception."); N.H. Rev. Stat. § 570-A:2(I) (prohibiting the interception of communications "without the consent of all parties to the

communication"); Wiretapping and Electronic Surveillance Control Act, 18 Pa. Stat. § 5704 (permitting the interception of communications only "where all parties to the communication have given prior consent to such interception.").

The Massachusetts Wiretap Act fits squarely into the continuum of laws that seek to protect communications privacy. To permit the otherwise unlawful interception of a private communication, the state Wiretap Act requires that the person listening in be "given prior authority by all parties to such communication." G.L. c. 272, § 99.

The phrase "[gave] prior authority," like the term "consent," signifies that the communicating parties (1) had sufficient information to make a true decision and (2) decided to grant permission for another to overhear their communication. See *Authorize*, Merriam-Webster (2015)[14] ("to give power or permission to (someone or something)"); *Permission*, Merriam-Webster (2015)[15] ("the right or ability to do

[14] http://www.merriam-webster.com/dictionary/authorize.
[15] http://www.merriam-webster.com/dictionary/permission.

something that is given by someone who has the power to decide if it will be allowed or permitted").

Further, it is apparent from the history of the Wiretap Act that the Legislature considered informed consent to be a core component of the statute. When legislators set out to revise the Act in 1968, one of their primary concerns was the revelation "that New England Telephone and Telegraph Company had been conducting 'service observations,' during which the company would secretly record private telephone calls to monitor service and customer perceptions of service." *Ennis*, 439 Mass. at 69. Following an investigation, the Special Commission on Electronic Eavesdropping condemned the telephone company for "clearly favor[ing] its business interest against right of the public to have privacy in their telephone conservations" and urged the Legislature "to insure that the privacy of the subscribers' telephone conversations [would] be protected." Special Commission Report, *supra* at 7. It concluded:

> The Commission is of the opinion that wiretapping and eavesdropping other than by law enforcement officers should be strictly prohibited. The present Massachusetts laws have been revised in our proposed act to strictly prohibit electronic eavesdropping

> and wiretapping of other persons' conversations *without permission*.

Id. at 9 (emphasis added).

The "prior authority" language of the Wiretap Act was thus largely intended to thwart unannounced "observations" by service providers with an informed consent requirement. The Legislature would not permit consent to be inferred merely because individuals continued to communicate through a service that might be subject to secret acts of monitoring–even if the *general practice* of monitoring was well-publicized. Rather, service providers, like all private parties, would have to obtain advanced permission before listening in on a communication.

III. There can be no actual knowledge of interception in this case because Google relies on secret algorithms to conduct its email data mining.

Logically, a person cannot give knowing consent to the interception of a communication without actually *knowing* that their communication is being intercepted. This Court underscored the point in *Jackson*: "[W]e accept . . . the proposition that the caller needs to have *actual knowledge* of the recording" *Commonwealth v. Jackson*, 370 Mass. 502, 507 (1976) (emphasis added). Actual knowledge is a high

bar; even a strong suspicion that a communication might be recorded is not enough if the party harbors any substantial doubts. See *Demoulas v. Demoulas Super Markets, Inc.*, 424 Mass. 501, 521 (1997) ("Massachusetts law does not equate suspicion with knowledge, and instead requires actual knowledge . . . where 'knowledge' of a fact means 'no substantial doubts as to its existence'" (internal quotation marks omitted)).

For example, a party might have "no substantial doubts" that a customer service call is being recorded if that fact stated clearly at the beginning of the call (e.g., "This call may be recorded for quality assurances purposes"). Such a disclosure would provide *specific* information about monitoring of an *individual* communication. See *also Jackson*, 370 Mass. at 507. But where, as here, a company has admitted to mining private communications data, but explicitly states that it does not inform users as to which messages it will mine, there can be no actual knowledge of interception.

Unlike a customer service line, Google does not warn outside senders that an individual communication is likely to be mined, nor does it give the sender an

opportunity to withhold consent. Instead, Google processes all communications, relies on a secret algorithm to mine some (but not all) messages for advertising purposes, and refuses to disclose–even after years of litigation on the subject–how that algorithm operates. See C.C. Dec. at 16. ("Google's systems do not provide any information to the non-Gmail sender that reflects scanning.").

The fact that Google has made general disclosures, alone, is not enough to require individual factual review of class member claims. Even if a class member had read every public statement, news story, court filing, and judicial opinion on the subject of Google's mining of private email data, they would still have no idea whether a particular communication would be mined-and the court would have no basis to conclude that they impliedly consented to such monitoring.

General knowledge of a broadly recurring practice is not actual knowledge of a *specific act*. Proceeding in the face of the former does not constitute consent to the latter, any more than wandering into a high-crime area implies consent to being mugged, or the mere existence of a corporate phone-monitoring policy

implies an individual employee's consent to eavesdropping. See *Williams*, 11 F.3d 271.

"Given algorithmic secrecy, it's impossible to know exactly" what companies are doing with personal data. Frank Pasquale, *The Black Box Society* 39 (2015). When a person does not actually know what a company is doing with their private communications, a court cannot infer that they have consented to some unknown practice. No degree of general awareness of Google's data mining practices can change this or establish consent by any individual class member. Knowledge of these general disclosures is simply irrelevant to the question of whether Google's mining of private email data constitutes interception under the Wiretap Act.

IV. Denying the extraterritorial reach of the Wiretap Act would undermine its privacy protections, hasten a data-mining race to the bottom, and leave Massachusetts law badly out of date.

If the court limits the Wiretap Act only to interception that occurs in Massachusetts, it will eviscerate protections for electronic communications and incentivize a race to the bottom where companies locate their processing centers in states with the weakest privacy protections. See Jenna Bednar, *The Political Science of Federalism*, 7 Ann. Rev. L. & Soc.

Sci. 269, 276 (2011) ("[W]ith policy decentralization comes the potential for a race to the bottom."). For example, if a company wished to mine the personal data and monitor the private communications of nonconsenting Massachusetts email users, it would need only to place the offending servers in one-party consent states and conduct its surveillance from those points. The most permissive state legislatures in the country would thus decide the level of privacy protection – if any – that Massachusetts users were entitled to in their electronic communications. See Matthiesen, Wickert, & Lehrer, S.C., *Laws on Recording Conversations in All 50 States* (July 11, 2016).

The absurdity of this scenario in an email context is clear by analogy to telephone calls:

> If businesses could maintain a regular practice of secretly recording all telephone conversations with their California clients or customers in which the business employee is located outside of California, that practice would represent a significant inroad into the privacy interest that the statute was intended to protect. . . . [A]n out-of-state company that does business in another state is required, at least as a general matter, to comply with the laws of a state and locality in which it has chosen to do business.

Kearney v. Salomon Smith Barney, Inc., 39 Cal. 4th 95, 126 (2006) (citations omitted); *see also Watson v. Employers Liab. Assur. Corp.*, 348 U.S. 66, 72 (1954) ("[M]ore states than one may seize hold of local activities which are part of multistate transactions and may regulate to protect interests of its own people, even though other phases of the same transactions might justify regulatory legislation in other states").

By contrast, if the Wiretap Act is enforced to its full extent and correctly applied to *all* interceptions of Massachusetts communications, the statute will serve to "ratchet up" privacy protections nationwide. See Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 Harv. J.L. & Pub. Pol'y 605 (2013) (describing the "ratcheting-up effect," wherein privacy protections in one jurisdiction "raise the privacy and security standards for all users, whether or not they have the benefit of [that jurisdiction's] legal rights"); David Vogel, *Trading Up: Consumer and Environmental Regulation in a Global Economy* 260-71 (1995) (explaining the "California effect," defined as the "ratcheting upward

of regulatory standards in competing political jurisdictions"). Rather than draining the Wiretap Act of its meaning in a world of rapidly evolving communications technology, a proper reading of the Act would place Massachusetts at the forefront of privacy protection and put positive pressure on other states to follow suit.

* * *

At issue in this case is the systematic data mining of millions of private email messages each day. The Wiretap Act cannot allow Google to intercept private communications and mine their contents for its own commercial purposes without consent. To do violates the purpose of the law.

CONCLUSION

Amicus Curiae respectfully request this Court to reverse the Superior Court's order granting summary judgment in favor of Google and reverse the Superior Court's denial of class certification.

Respectfully submitted,

Marc Rotenberg (BBO# 550488)
Caitriona Fitzgerald (BBO# 673324)
Alan Butler
Electronic Privacy Information
Center (EPIC)
1718 Connecticut Ave. NW
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

October 24, 2016

Mass. R. A. P. 16(k) CERTIFICATION

I hereby certify that the above brief complies with the rules of court that pertain to the filing of briefs, including, but not limited to: Mass. R. A. P. 16(a)(6); Mass. R. A. P. 16(e); Mass. R. A. P. 16(f); Mass. R. A. P. 16(h); Mass. R. A. P. 18; and Mass. R. A. P. 20.

/s/ Caitriona Fitzgerald
Caitriona M. Fitzgerald
BBO# 673324
Counsel for *amicus curiae* EPIC