IMPOUNDED

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION
No. 11-2808-BLS1

DEBORAH L. MARQUIS

vs.

GOOGLE, INC.

****

MEMORANDUM AND ORDER ON CROSS-MOTIONS FOR SUMMARY JUDGMENT

This action tests whether Google, in its automated scanning of emails sent between Gmail accounts and non-Gmail accounts – in significant part to facilitate targeted or personalized advertising directed at Gmail users – violates Massachusetts' wiretap statute, G.L. c. 272, §99. Because I conclude that the statute does not apply to the extraterritorial conduct at issue, Google's motion to dismiss the complaint is allowed.

FACTS

The following facts are not subject to genuine dispute. Gmail is a web-based email service that Google provides without charge to more than 69 million Americans and hundreds of millions worldwide. The plaintiff uses an AOL email platform, but she sends and receives emails to and from Gmail accounts.[1]

---

[1]The case was filed as a class action. On June 19, 2014, the Court (Kaplan, J.) denied the motion for class certification, "except with respect to a possible class of non-Gmail email users that exchanged emails with an email user whose email service was provided by a Google Apps customer who permitted targeted advertising; and as to such a possible class, the court [made] no ruling." The issue has not been pursued further.

From the time that Gmail was launched in 2004, Google has used automated technologies to scan emails received by Gmail users and, at times, emails sent from Gmail accounts. These enable Google to provide "targeted" or "personalized" advertising (for the difference, see below) to Gmail users. This generates revenue for Google, at least some of which goes to offset the cost of providing Gmail for free.[2] Scanning emails also facilitates services unrelated to advertising that reduce cost, increase efficiency, and enhance the user experience. These include detection and interruption of spam, viruses and "phishing" emails; implementation of user-created filters; automated categorization of emails; enabling the user to search within the account for keywords; identifying dates to facilitate reminders on the user's Google calendar; and identifying shipping notifications so that the user may click a button to fetch package tracking information.

Google's methods of scanning emails, then using the results to select targeted or personalized advertising, have evolved with the passage of time. Until [redacted] – and since then to the present day, but to a much lesser extent – Google has used what will be referred to herein as the [redacted] process. Once an incoming email has been [redacted] The results are then forwarded to a [redacted] which

[2]The other major email platforms also use some form of targeted advertising. The largest in the U.S. – Yahoo! – informs its users that it provides personally relevant features, content and advertising by scanning and analyzing the content of Mail!, Messenger, and other communications. Microsoft and AOL have also publicized the fact that they target advertising using, in part, information gleaned from use of their sites; this includes users' search patterns and other data but not, apparently, message content.

[3]These three requirements – [redacted] – mean that not all emails sent to Gmail accounts were (or are) scanned. Roughly [redacted]

processes the information, looking for keywords that are then used in selecting advertisements to be displayed to the user as he or she views the email.

Google's term for this is "targeted advertising." In specific circumstances, Google also scans outgoing emails, then directs the Gmail user to the Inbox where an ad based on the just-sent email is displayed.

[redacted] processing is automated and does not involve human review. Neither the sender nor the recipient of an email involving a Gmail account is notified that Google has scanned it.

In or about [redacted], Google implemented a new system called "User Modeling" or "Personalized Advertising." User Modeling has largely but not entirely supplanted the [redacted] system, which remains in limited use. A server using Google's Content Onebox ("COB") technology scans the text of emails sent to a Gmail user for keywords and other information that can be used to select advertising likely to be relevant to the Gmail user's interests.[4] [redacted] At times, the system has then added to the incoming email's metadata stored on Google servers, but not to the message

---

[redacted] see text below). Other issues may [redacted] Many of these exceptions are beyond the control of the email's sender, and none are particularly germane to the legal issues presented here.

[4]As with the [redacted], there is content that COB [redacted]

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

[redacted] uses the information gathered from COB scanning as well as other factors to construct the GMail user's "User Model." This is based on the user's most recent emails. Most information in a User Model [redacted] User Modeling is used to select for Gmail users what Google calls "personalized advertising," selected to correspond with what the User Model suggests are the user's interests. As with the [redacted] all of this is done through a series of automated steps on large servers, not human review.[5]

All of the scanning processes that implement targeted or personalized advertising are implemented on servers located outside of Massachusetts. The code that implements the [redacted] is run on servers physically located in [redacted]. The code that implements the COB process is run on servers physically located in [redacted] The code that implements the User Model process is run on servers physically located in [redacted] None of the processing occurs in Massachusetts.

---

[5]A Gmail user may opt out of personalized advertising. In that case, a COB server will [redacted]

Google's "Create and Account" page (see below) does not require or permit an accountholder to provide his or her state of residence. Nor is there any reliable way for Google to determine the residence of a non-Gmail user who sends an email to, or receives one from, a Gmail account.[6]

Although Google is highly protective of its proprietary information concerning scanning protocols – hence, the likelihood that the publicly released version of this decision will contain some redactions – the fact that it scans emails and uses the results to correlate advertising with subscribers' interests has been widely publicized, to Gmail users and others. Since at least 2008[7] the "Create An Account" page by which users sign up for Gmail has explained,

> With Gmail, you won't see blinking banner ads. Instead, we display ads you might find useful that are relevant to the content of your emails.

This is immediately followed by a link by which the would-be subscriber is invited to "Learn more" by viewing a page titled "Ads in Gmail and your personal data." This begins:

---

[6]A Google witness was questioned at some length whether an incoming email came with the sender's IP address as metadata; if so, whether this would enable to determine the physical location of the internet connection from which the email was sent; and if so, how accurately. The didn't know the answer to any of these questions, on which the record is otherwise silent, and neither do I. The plaintiff's response – that perhaps voter lists would be of assistance – may have been germane to the question of class certification, but it has little relevance to the issue at hand. Although I take judicial notice of the fact that police officers have been able to subpoena account information from the internet service provider that supplied a known IP address, this is not to say that Google could do this in real time, or without a subpoena. Finally, Gmail is a web-based platform that may be accessed from any computer or mobile device; even knowing the precise physical address from which an email was sent is not the same thing as knowing the sender's state of residence.

[7]Google's disclosures, like the technology and its use, have evolved over time. Current versions are available to all on line, and prior versions of some are similarly available on "archive" pages.

How Gmail Ads Work

> Ads that appear next to Gmail messages are similar to ads that appear next to Google search results and on content pages throughout the web. In Gmail, ads are related to the content of your messages. Our goal is to provide Gmail users with ads that are useful and relevant to their interests.
>
> Ad targeting in Gmail is fully automated, and no humans read your email in order to target advertisements or related information. This type of automated scanning is how many email services, not just Gmail, provide features like spam filtering and spell checking. Ads are selected for relevance and served by Google computers using the same contextual advertising technology that powers Google's AdSense program [another link].

Google's Terms of Service and Privacy Policies – to which all subscribers must acknowledge and agree when creating a Gmail account – also disclose in general fashion that Google collects data from users, and specify that Google will use data only to provide its services, develop new services, and for security reasons. For example, the Terms of Service document in place from April 2007 until March 2012 stated:

> Some of the Services are supported by advertising revenue and may display advertisements and promotions. These advertisements may be targeted to the content of information stored on the Services, queries made through the Services or other information.

Services are defined as, "Google's products, software, services and web sites." Since March 2012, the successor document has said,

> Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies.

The current Google Privacy Policy advises users that Google collects information regarding how they use Google services, and that it "use[s] this information to offer you tailored content – like giving you more relevant search results and ads."

From at least October 14, 2005 to October 3, 2010, Google also maintained a separate Gmail Privacy Policy, which disclosed explicitly that Google processes emails in order to provide various features of Gmail. For example, a link to a "Gmail Privacy Notice" from the navigation bar in the Google Privacy Policy dated October 14, 2005 advised,

> Google maintains and processes your Gmail account and its contents to provide the Gmail service to you and to improve our services. The Gmail service includes relevant advertising and related links based on the IP address, *content of messages* and other information related to your use of Gmail. Google's computers process the information in your messages for various purposes, including formatting and displaying the information to you, delivering advertisements and related links, preventing unsolicited bulk email (spam), backing up your messages, and other purposes relating to offering you Gmail. (Emphasis supplied.)

Google's website has "Help" pages and Google tools that allow users to customize their privacy and advertising settings. The language of the Help pages has changed over time. One is the "Ads in Gmail and your personal data" page linked to the "Create and Account page and quoted above. This Help page received over [redacted] views from 2010 to 2012.

From December of 2011 to December of 2012, another Help page had the following:

> Is Google reading my mail?
>
> No, but automatic scanning and filtering technology is at the heart of Gmail. Gmail scans and processes all messages using fully automated systems in order to do useful and innovative stuff like filter spam, detect viruses and malware, show relevant ads, and develop and deliver new features across your Google experience. Priority Inbox, spell checking, forwarding, auto-responding,

> automatic saving and sorting, and converting URLs to clickable links are just a few of the many features that use this kind of automatic processing.

All of this information, of course, is directed at Gmail users. Although Google's Terms of Use or Privacy Policies are readily available on line, they are not explicitly directed at non-Gmail users.

Since the 2004 launch, however, numerous major and not-so-major media outlets have reported extensively – some favorably, some not – on Gmail's automated scanning feature and its use in facilitating targeted or personalized advertising.[8] An email recipient or sender who had encountered the media coverage, and noticed that the correspondent's email address ended in ".gmail," might make the connection, or might not. In fact the plaintiff, a resident of Boxford, Massachusetts with an AOL email account, did not realize that her emails to Gmail accounts were being scanned until shortly before her complaint was filed on July 29, 2011.

Even a sender who knows that Google scans emails sent to and from a Gmail account, moreover, may not know that a particular correspondent is using Gmail, because not all Gmail accounts have "@gmail" addresses. Google Apps, a suite of productivity and collaboration tools and software – including a version of Gmail – is offered on a subscription basis to businesses,

---

[8]Judge Kaplan's class certification decision summarizes facts concerning media coverage found in a declaration of Kyle Wong dated January 17, 2014, which was submitted with the certification motion papers but not with the summary judgment papers. See Memorandum of Decision and Order on Plaintiff's Motion for Class Certification (Papers #48, #49; Kaplan, J.), pp. 6-8.

Of particular interest locally is a column by Hiawatha Bray in the May 31, 2004 Boston Globe titled, "Google's Gmail Is Still a Rough Draft." In Bray's estimation, "Google's plan to make money off the [Gmail] service by featuring ads inspired by the contents of the e-mail messages" was "[n]ot really" intrusive; "Indeed, it's sort of cool. ... Unlike most ads, these relate to something that interests you, so you'll almost certainly read them."

educational organizations, and internet service providers, and allows subscribers to use their own domain name (e.g., @yourcompany.com, @yourcollege.edu, etc.). Someone corresponding with an employee at a company or institution that subscribes to Google Apps, therefore, would not know from the email address that this is a Gmail account.[9]

In short: regardless of Google's disclosures to its Gmail accountholders and general knowledge derived from press accounts, one may not assume that all of those with whom those accountholders correspond by email – including, before July 2011, the plaintiff – are aware that some of the correspondence will likely be subject to an automated scanning process.

DISCUSSION

A. The Massachusetts Wiretap Statute.

The Massachusetts wiretap statute, G.L. c. 272, §99, has its antecedents in Chapter 558 of the Statutes of 1920. It substantially rewritten in 1959 and again in 1968. Since then, there have been only minor and, for present purposes, irrelevant revisions in 1986, 1993, and 1998, described in the margin.[10] For present purposes, therefore, the statute is effectively 46 years old, and has

---

[9]Google Apps' email function has other features that differentiate it from a stand-alone Gmail subscription. For example, the system administrator of the entity subscribing to Google Apps determines the content and implementation of terms of service, use policies, or privacy policies associated with end user accounts, including whether and how the user may opt in or out of advertising.

[10]The 1986 amendment was purely technical, removing the redundant figure "($10,000)" in subpart C.2's imposition of a criminal fine of ten thousand dollars for tampering with the transcript of a judicial proceeding. In 1993, subpart D.1.e was added, permitting law enforcement officer and agents to wear wires to ensure their safety; the amendment also specified that "the law in effect at the time an offense is committed shall govern sentencing for such offense." The 1998 amendment, by adding subparts B.17, B.18, and D.1.f, added "ordinary course of business" exemptions specific to the financial industry.

remained materially unchanged since well before the advent of personal computers, the Internet, internet advertising, and web-based email.

The statute as now written provides that

> any person who ... willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment.

G.L. c. 272, §99.C.1.[11] Subsection Q additionally provides for civil remedies for an unlawful interception, including actual damages or liquidated damages in the higher amount of $100 per day of violation or $1000, punitive damages, and attorneys' fees and costs. The statute does not distinguish between conduct that is punishable criminally and that which is subject to civil remedies; an act either is an unlawful interception, or it isn't.

Central to the statute is the definition of "interception," which contains a "one-party consent" exception for law enforcement officials investigating certain "designated offenses" enumerated elsewhere in the statute:

> The term "interception" means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication; provided that it shall not constitute an interception for an investigative or law enforcement officer, as defined in this section, to record or transmit a wire or oral communication if the officer is a party to such communication or has been given prior authorization to record or transmit the communication by such a party

---

[11] Additional offenses under the statute include disclosure or use of unlawfully intercepted communications, possession of an interception device, and aiding and abetting an unlawful interception. G.L. c. 272, §99.C.2-6.

> and if recorded or transmitted in the course of an investigation of a designated offense as defined herein. (G.L. 272, §99.B.4.)

An exemption at G.L. c. 272, §99.D.1.d additionally allows law enforcement to engage in non-consensual interceptions authorized by a warrant.

Massachusetts' is thus, at least where civilians are concerned, a two-party consent law, in that consent to an otherwise prohibited interception must be given by "all parties to [the] communication." This distinguishes the Massachusetts law from the federal Electronic Communications Privacy Act of 1986 (ECPA), Pub.L. 99-508, 100 Stat. 1848 (1986), (codified at 18 U.S.C. §2511 and elsewhere)[12] and most state wiretap statutes,[13] which permit interceptions with the consent of just one party.

Several of the other statutory definitions and the exceptions embedded therein are potentially germane to this case. They include the following:

> The term "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception. (G.L. 272, §99.B.1.)

---

[12]The ECPA permits interceptions by a civilian party "where such person is a party to the communication or where *one of the parties* to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. §2511(2)(d) (emphasis supplied).

[13]Thirty-eight states plus the District of Columbia have one-party consent laws, while eleven – California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania and Washington – have various sorts of two-party consent statutes. See Digital Media Law Project, "Recording Phone Calls and Conversations," available at: http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations. The Illinois statute was recently ruled unconstitutionally overbroad and violative of the First Amendment. People v. Melongo, 2014 IL 114852, 379 Ill. Dec. 43, 6 N.E.3d 120 (Ill. Supr. 2014).

****

> The term "intercepting device" means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and *other than* any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business. (G.L. 272, §99.B.3; emphasis supplied)

****

> The term "communication common carrier" means any person engaged as a common carrier in providing or operating wire communication facilities. (G.L. 272, §99.B.12.)

The parties appear to agree that because the internet depends on cable connections, emails constitute "wire communications." Google argues, however, (1) that the "ordinary course of business" exception to the statutory definition of an "intercepting device" (G.L. 272, §99.B.3) applies to both the [redacted] and the User Model process; (2) that the [redacted] is additionally exempted because scanning emails after they reach the recipient is not an "interception" within the meaning of (G.L. 272, §99.B.4); (3) that the scanning, having taken place outside of Massachusetts, is not subject to the Massachusetts wiretap statute in any event; and (4) that if all else fails, the plaintiff is at least barred from claiming relief for scanning that occurred after she became aware of the practice.

Because I conclude that the statute does not apply to an interception occurring outside Massachusetts, it is unnecessary to reach the other issues Google has raised, other than to note that each raises interesting and, at times, challenging issues of statutory construction. These are

especially apparent in the "ordinary course of business" defense and emanate in part – but only in part – from the fact that unlike the federal ECPA, the Massachusetts statute has remained fundamentally unchanged since 1986, and so has occasionally undergone awkward but necessary judicial updating to "'maintain its viability in the broad run of cases'" while keeping pace with changes in technology and commerce. Commonwealth v. Moody, 466 Mass. 196, 207 (2013), quoting Dillon v. Massachusetts Bay Transp. Auth., 49 Mass. App. Ct. 309, 314-16 (2000).

B. Extraterritorial Application of the Massachusetts Wiretap Statute.

As noted above, the servers on which Google scans emails of Gmail users are physically located in [redacted] None are located in Massachusetts, and so no interceptions physically occur within our borders.

In a series of criminal and civil cases, Massachusetts and federal courts have declined to apply the Massachusetts wiretap statute to interceptions occurring outside Massachusetts. The sole appellate precedent on the issue is Commonwealth v. Wilcox, 63 Mass. App. Ct. 131, 139 (2005). There, the defendant gave a statement in a Rhode Island police station that the interrogating officer recorded without his knowledge. The Appeals Court upheld the trial court's denial of a motion to suppress the statement, noting that "[t]he defendant cites no authority for the proposition that G.L.

---

[14]It may not be coincidental that these are all one-party consent jurisdictions (see footnote 13, *supra*). Nonetheless, at least one court has, in ruling on a motion to dismiss, found that Gmail users' acceptance of Google's Terms of Service and Privacy Policies "does not establish explicit consent" even on the part of Gmail accountholders, because these documents are insufficiently explicit as to what Google does and how it uses the information thus obtained. In re: Google, Inc. Gmail Litigation, 2013 WL 5423918 (U.S. Dist. Ct., N.D. Cal., Sept. 26, 2013) at *12-*15. One might debate the point, but the federal court's further holding "that non-Gmail users who are not subject to Google's Privacy Policies or Terms of Service have [not] impliedly consented to Google's interception of their emails to Gmail users" (id. at *14) seems all but irrefutable. Google has not advanced a consent argument in this case.

c. 272, § 99, applies to recordings made outside of Massachusetts." Similarly, in Commonwealth v. Tibbs, 2007 WL 4644818 (Mass. Super. 2008; Gants, J.), a judge then of this Court, citing Wilcox, ruled admissible statements made in a Rhode Island jail by the defendant to a detainee secretly wearing a wire.

Closer to the present case on its facts, in that it concerned an interstate wire communication originating in Massachusetts and intercepted elsewhere, is Commonwealth v. Maccini, 2007 WL 1203560 (Mass. Super. 2007; Fabricant, J.). There, the defendant sent emails and instant messages from Massachusetts to a person who, unbeknownst to the sender, was the Chief of Police of the New Waterford, Ohio, Police Department, and was conducting an undercover investigation into trading of child pornography on the internet. The Chief saved the communications, which were then used in a Massachusetts investigation to obtain warrants to search the defendant's AOL account and his computers. Holding that the Massachusetts wiretap statute did not apply, the court remarked:

> A fundamental characteristic of the federal system is that each state is entitled to its own laws, subject to the supremacy of federal law, but that no state may impose its laws on another. See generally, Commonwealth v. Aarhus, 387 Mass. 735, 742 (1982). Massachusetts has not purported to do so; nothing in the wiretap statute suggests any intention to regulate conduct outside the bounds of the Commonwealth. See Commonwealth v. Wilcox, 63 Mass. App. Ct. 131, 139 (2005). Federal law permits recording with the consent of one party to the communication. See Commonwealth v. Blood, [400 Mass. 61, 67 (1987)], citing United States v. Caceres, 440 U.S. 741, 750-751 (1979), and United States v. White, 401 U.S. 745, 751 (1971). The defendant has identified no Ohio statute or other authority that would prohibit [Chief] Haueter's conduct, and at argument conceded that none exists. Thus, Haueter's conduct violated no law, and was not "unlawful" within the meaning of c. 272, §99P1. For that reason alone, the defendant's motion to suppress must be denied.

Id. at *2.

At least two federal cases have reached the same conclusion in civil cases brought under the Massachusetts statute. In MacNeil Engineering Co. v. Trisport, Ltd., 59 F. Supp. 2d 199, 202 (D. Mass. 1999; Young, J.), the defendant recorded in England a telephone call originating in Massachusetts. And in Pendell v. AMS/Oil, Inc., 1986 WL 5286 (D. Mass. 1986; Collings, U.S.M.J.) at *4, the reverse occurred: a Rhode Island caller recorded his telephone call to a Massachusetts recipient. In both cases, the holding was that the Massachusetts statute did not apply to the out-of-state interception.

On the other hand, at least one decision from this Court, noting the lack of binding precedent and applying principles drawn from the Restatement (Second) of Conflict of Laws, has applied the statute to an interstate telephone call emanating in Massachusetts and recorded by the recipient in Virginia. Heffernan v. Hashampour, 2009 WL 6361870 (Mass. Super. 2009). The facts in the present case, however, underscore the wisdom of the Maccini, MacNeil Engineering and Pendell holdings, particularly when one leaves the era of old-style telephones and enters the Internet Age.

Emails are distinctly unlike land-line telephone calls in many respects, one being that an email may be sent or received anywhere that has an internet or cellular connection, using highly portable equipment – laptops with WiFi connections, tablets, and mobile phones. They travel from one @-sign "address," wholly unrelated to any geographic location, to another.

As noted above, Google does not keep a record of a Gmail user's residential address. More to the point, Google has no way of knowing where the accountholder's correspondent – the plaintiff in this case, for example – resides. Nor is there evidence that Google could know where either was situated when sending or receiving a particular email (see footnote 5), an issue on which, to whatever extent it may be relevant, the plaintiff has the burden of proof.

Applying the Massachusetts wiretap statute to Gmail communications sent to or from a Massachusetts resident or visitor – irrespective of where they might be scanned or processed – would thus make compliance a game of chance. Assuming that no responsible entity would risk a Massachusetts felony prosecution by scanning an email that *might* have been sent or received in Massachusetts or by a Massachusetts resident, the practical effect would be to regulate the practice nationwide. Some would undoubtedly view this as a desirable result; others would just as surely disagree. In either event, "a State may not impose economic sanctions on violators of its laws with the intent of changing the tortfeasors' lawful conduct in other States." BMW of North America, Inc. v. Gore, 517 U.S. 559, 573 (1996).

"A fundamental tenet of statutory interpretation is that statutory language should be given effect consistent with its plain meaning and in light of the aim of the Legislature unless to do so would achieve an illogical result." Sullivan v. Brookline, 435 Mass. 353, 360 (2001). The Massachusetts wiretap statute says nothing, one way or the other, about extraterritorial application. Federal regulation is one thing,[15] see Gore at 572, but there is no reason to suspect that the Massachusetts legislature intended, in 1968 or since, that our statute be applied to out-of-state conduct, especially where this would amount to a Massachusetts-imposed interdiction against a practice whose implementation occurs elsewhere and whose effects – good and bad – are worldwide.

---

[15]As it happens, a federal court in California is considering the legality of Google's scanning and processing of emails under the federal ECPA, as well as California's wiretap statute. In re: Google, Inc. Gmail Litigation, 2013 WL 5423918 (U.S. Dist. Ct., N.D. Cal., Sept. 26, 2013). So far, the plaintiffs have survived a motion to dismiss but lost their motion for class certification. The case is still pending.

The statute's criminal penalties are relevant for another reason as well. "The general rule, accepted as 'axiomatic' by the courts in this country, is that a State may not prosecute an individual for a crime committed outside its boundaries." Vasquez, petitioner, 428 Mass. 842, 848 (1999); see cases cited there and in Commonwealth v. Armstrong, 73 Mass. App. Ct. 245, 249 (2008).

To this general rule there is the narrow exception known as the "effects doctrine," under which "[a]cts done outside a jurisdiction, but intended to produce and producing detrimental effects within it, justify a State in punishing the cause of the harm as if he had been present at the effect." Strassheim v. Daily, 221 U.S. 280, 285 (1911; Holmes, J.).[16] Assuming that users of non-Gmail accounts are detrimentally affected by Google's out-of-state scanning of emails, Google cannot be said to have "intended to produce" such effects within Massachusetts when it had no way of knowing where the sender or recipient of a particular email was located. As the Appeals Court observed in Armstrong, the effects doctrine is not "so broad as to empower a State to exercise jurisdiction where all acts in furtherance of the crime and all offense elements of the crime are committed wholly outside the borders of the State." 73 Mass. App. Ct. at 251.

For all of these reasons, I very much doubt that the Legislature, in 1986 or since, intended that the wiretap statute be applied to the out-of-state conduct at issue here. Google's Motion for Summary Judgment is therefore allowed.

---

[16]In Strassheim the respondent, a Chicago businessman, traveled to Michigan – the prosecuting jurisdiction – to deliver a bid, which a state authority signed in his presence, for the purchase of $10,000 worth of new equipment; what was later delivered, however, was secondhand equipment. In Vasquez, the SJC applied the Strassheim rule to a Massachusetts father's failure to pay child support to his family in Oregon.

ORDER

For the foregoing reasons, the defendant's Motion to Dismiss is ALLOWED. Judgment to enter, dismissing the Complaint. The text of this decision other than the Order shall be impounded pending decision on any motion (joint if possible) for redaction, to be filed with a copy of the proposed redacted decision within 20 days of the date the Order is docketed.

Thomas P. Billings
Justice of the Superior Court

Dated: February 13, 2015