STOP THE ABUSE OF GMAIL!

GRANT YANG[1]

ABSTRACT

Gmail, a highly anticipated webmail application made by Google, has been criticized by privacy advocates for breaching wiretapping laws, even before its release from beta testing. Gmail's large storage space and automated processes developed to scan the content of incoming messages and create advertisements based on the scanned terms have enraged privacy groups on an international level. This iBrief will compare Gmail's practices with its peers and conclude that its practices and procedures are consistent with the standards of the webmail industry. The iBrief will then propose additional measures Gmail could institute to further protect webmail users' and alleviate the concerns of privacy advocates.

INTRODUCTION

¶1 Louis Gerstner, former CEO of IBM, once stated that with new technology the "real issues are not technical;" rather, the benefit stemming from new technology "is always counterbalanced by an equally important list of societal concerns."[2] Though not officially released to the general public, Google's webmail client, Gmail, illustrates Gerstner's statement, as it has already generated not only praise and excitement, but also criticism and threats of legislative regulation.

¶2 Two components of Gmail that raise privacy concerns are its two-gigabyte storage capacity and its Adsense technology, which scans e-mail and places advertisements into the message related to its content.[3] This iBrief will analyze Gmail's conformity with privacy laws and compare Gmail to other webmail clients such as Yahoo! and MSN Hotmail ("Hotmail"). Section I will begin by providing the history of Gmail and the Adsense technology. Section II will then analyze Gmail's expanded data storage capacity and its legal and practical implications. Section III will address concerns specifically related to the Adsense technology, its

---

[1] B.S. in Computer Science, Stanford University, 2001; Candidate for J.D., Duke University School of Law, 2005; Candidate for LL.M. in International and Comparative Law, Duke University School of Law, 2005.

[2] LOUIS V. GERSTNER, JR., WHO SAYS ELEPHANTS CAN'T DANCE? 272 (HarperCollins 2003) (2002).

[3] *About Gmail*, GMAIL, *at* http://gmail.google.com/gmail/help/about.html (last visited Oct. 10, 2004).

compliance with current statutes, threatened regulation, and implications on society's collective expectation of electronic privacy. Finally, section IV will present several options for Google to consider that may alleviate some of these privacy concerns.

I. BACKGROUND

¶3 Since its founding in 1998,[4] Google has become an economic powerhouse, capturing the largest market share of the Internet search industry.[5] Like many search providers, Google is expanding its services to include webmail, an e-mail application that is more convenient and accessible for mobile consumers than traditional e-mail clients.[6] Eventually Google hopes to integrate its many different services,[7] including webmail, to create a profitable product.

¶4 Gmail's innovative features have turned heads in the technology community. The free service originally included one gigabyte of storage space;[8] a significantly larger amount than search engine rivals Yahoo! and MSN offered.[9] However, Gmail recently announced it would double

---

[4] *Google History*, GOOGLE, *at* http://www.google.com/corporate/history.html (last visited Oct. 10, 2004).

[5] Danny Sullivan, *comScore Media Metrix Search Engine Ratings*, SEARCHENGINEWATCH, July 23, 2004, *at* http://searchenginewatch.com/reports/article.php/2156431 (Google has 36.8% as of May 2004).

[6] Brad Templeton, *Privacy Subtleties of Gmail*, *at* http://www.templetons.com/brad/gmail.html (last visited Oct. 10, 2004). Some services can be comprehensive, such as .Mac, which for $99 per year, offers an e-mail account with virus protection, backup software, online file storage, calendar synching, web hosting, web-design tools, and system backups. Alex Salkever, *Can .Mac Withstand the G-Force*, BUSINESSWEEK ONLINE, Apr. 15, 2004, *at* http://www.businessweek.com/technology/content/apr2004/tc20040415_8968.htm.

[7] *See About Orkut*, *at* http://www.orkut.com/about.html (last visited Oct. 10, 2004) (describing Google's online network software that applies the six-degrees of separation concept of networking); Amit Asaravala, *Google to Unveil Free E-mail*, WIRED, Mar. 31, 2004, *at* http://www.wired.com/news/business/0,1367,62897,00.html (describing Gmail and the Google search engine).

[8] Asaravala, *supra* note 7.

[9] *See* Evan Hansen, *The Fellowship of the 1GB Storage Lockers*, CNET NEWS.COM, May 27, 2004, *at* http://news.com.com/The+fellowship+of+the+1GB+storage+lockers/2100-1024_3-5221988.html (describing how Yahoo and Lycos boosted their storage); Graeme Weardon, *Lycos: We're First with a Gigabyte of E-Mail*, CNET NEWS.COM, May 18, 2004, *at*

storage capacity to two gigabytes.[10] Gmail also indexes messages using Google's search technology, allowing users to search their stored e-mail based on key terms rather than traditional organizing methods such as date and sender.[11] A further innovation of Gmail is that it arranges messages in conversation threads.[12] The threads allow users to view e-mails and their responses as an entire conversation chain rather than as individual messages.[13]

¶5 Unlike its rivals, Gmail does not display randomly generated banner or popup advertisements.[14] Instead, Gmail couples its Adsense technology[15] with its search engine[16] to place text-based ads into the content of e-mail messages. Adsense, a wholly automated process, scans the content of incoming e-mail messages for key words and selects advertisements

---

http://news.com.com/Lycos%3A+We%27re+first+with+a+gigabyte+of+e-mail/2100-1024_3-5214626.html (stating that Lycos announced it would offer 1 gigabyte of storage). MSN charges $19.95 a year for 2 gigabytes of storage. *MSN Hotmail Plus*, MSN, *at* http://join.msn.com/content.aspx?pgmarket=en-us&page=hotmail/es&ST=1&xAPID=1983&DI=1402 (last visited Oct. 9, 2004). Yahoo! recently announced that it planned to boost its free e-mail limit to 1 gigabyte. Jim Hu, *Yahoo Bolsters E-Mail Storage to 1GB*, CNET NEWS.COM, Mar. 22, 2005, *at* http://news.com.com/Yahoo+bolsters+e-mail+storage+to+1GB/2100-1032_3-5630773.html?tag=nefd.top.

[10] Evan Hansen, *Google Plans to Double Gmail Capacity—At Least*, CNET NEWS.COM, Mar. 31, 2005, *at* http://news.com.com/Google+plans+to+double+Gmail+capacity--at+least/2100-1032_3-5649571.html?tag=nefd.top.

[11] Letter from Marcia Hoffman, Staff Counsel, Electronic Privacy Information Center, to David M. Hardy, Chief, Records/Information Dissemination Section of the Federal Bureau of Investigation (Apr. 29, 2003), *at* http://www.epic.org/privacy/gmail/foirequest.html. To view screenshots of search capabilities, see http://gmail.google.com/gmail/help/screen3.html.

[12] *About Gmail*, *supra* note 3; Steve Gillmor, *Google's Brin Talks on Gmail Future*, EWEEK.COM, Apr. 23, 2004, *at* http://www.eweek.com/article2/0%2C1759%2C1572683%2C00.asp.

[13] *Getting Started With Gmail*, GMAIL, *at* http://gmail.google.com/gmail/help/start.html (last visited Oct. 10, 2004).

[14] *See* Kim Zetter, *Free E-mail With a Steep Price?*, WIRED, Apr. 1, 2004, *at* http://www.wired.com/news/business/0,1367,62917,00.html (describing its advertising method of placing text ads).

[15] Adsense automatically delivers text and image ads "that are precisely targeted, on a page-by-page basis, to [a] . . . site's content." *Google Adsense for Content*, GOOGLE, *at* https://www.google.com/adsense/afc-online-overview (last visited Oct. 10, 2004). Google Adwords also allows customers to create their own ads, choose keywords to match ads, and pays per click. *Google Adword*, GOOGLE, *at* https://adwords.google.com/select/Login2 (last visited Oct. 10, 2004).

[16] *See Google AdSense FAQ*, GOOGLE, *at* https://www.google.com/adsense/faq (last visited Oct. 10, 2004) (describing the program and its use with Google).

corresponding to the words. However, Google maintains that no human ever reads the content of incoming e-mails.[17] Wayne Rosing, Google's vice president of engineering, has publicly stated that Google will not sell ads based on certain sensitive words, nor will it keep a record of keywords that appear in an individual's e-mail.[18]

II. DATA STORAGE, COMPLIANCE AND LAW ENFORCEMENT

¶6 Critiques of Gmail have attacked the system on a number of fronts. The most frequent criticisms focus on the privacy dangers associated with the large storage capacity and linking tools.

A. Risks of Data Storage and Linkage

¶7 Consolidated data storage is generally risky, especially on third-party servers. History provides a long list of compromised e-mail servers and divulged secrets.[19] Privacy advocates are concerned that Gmail's large storage space will encourage users to consolidate all their data in a Gmail account and retain e-mail messages for longer periods of time.[20] If hacked, an unauthorized user could create a "detailed portrait" of a user's life.[21]

---

[17] *Gmail and Privacy*, GMAIL, *at* http://gmail.google.com/gmail/help/more.html (last visited Oct. 10, 2004). The terms-of-service agreement clearly states that the ad targeting is done by machines. Asaravala, *supra* note 7. Although the Terms of Service do not describe the ad-placement, Gmail's privacy policy does. *Gmail Privacy Policy*, GMAIL, *at* http://www.google.com/gmail/help/privacy.html (last visited Oct. 10, 2004).

[18] Zetter, *supra* note 14.

[19] Declan McCullagh, *Is Google the Future of Email?*, CNET NEWS.COM, Apr. 12, 2004, *at* http://news.com.com/Is+Google+the+future+of+e-mail%3F/2010-1032_3-5187543.html (listing both Yahoo! and Hotmail as victims of bugs in their security). Already, while still in its testing phase, Gmail has fixed a security flaw that would have allowed a hacker to steal a victim's cookie file and gain access to the user's e-mail account. John Leyden, *Google Blocks Gmail Exploit*, THE REGISTER, Nov. 1, 2004, *at* http://www.theregister.co.uk/2004/11/01/gmail_bug_fixed/.

[20] Some users store not only their e-mail data, but also various other types of common Internet data. Coders have created hacks for Gmail, including using Gmail to serve as an online drive and also as a blog service. *See Gmail Drive Shell Extension*, VIKSOE.DK, Oct. 4, 2004, *at* http://www.viksoe.dk/code/gmail.htm (allowing users to create a virtual file system using Gmail); Jonathan Hernandez, *Gallina: Just a Gmail Based Blog*, *at* http://ion.gluch.org.mx/files/Hacks/gallina/ (last visited Oct. 28, 2004) (using the e-mail entries as Gmail blog messages with comment and picture support).

[21] Stephen H. Wildstrom, *Google's Gmail is Great – But Not for Privacy*, BUSINESSWEEK ONLINE, May 3, 2004, *at* http://www.businessweek.com/@@lxHQa2QQkU7dcRAA/premium/content/04

This risk, however, is prevalent in many webmail services; some which provide even more than Gmail's two gigabytes of storage.

¶8 While Gmail servers operate in separate clusters from Google's other services, Google is considering linking their functionality so users can learn of new e-mail when performing a Google search.[22] Despite the increased efficiency of such a system, it does not come without risks. Such a linking system would require Google to store both Gmail and user preferences on a single cookie.[23] If a hacker ever gained access to the cookie, he could link stored e-mails with web surfing history, creating a complete profile of a user. Given the potential risks, linking between webmail and other Internet services should be heavily scrutinized.

B. Data Retention and the European Union Privacy Directive

¶9 Privacy International, along with thirty-one other privacy groups, charges that Gmail's server backup policies violate the E.U. Privacy Directive[24] by storing messages "where users cannot permanently delete them."[25] Specifically, the Directive requires Internet Service Providers (ISP) to give users greater control over their communications and refrain from storing data longer than necessary.[26] In the United Kingdom, for example, the key inquiry when addressing potential Directive violations focuses on the data controller's need "to keep the information . . . when the relationship [between the data controller and user] ceases to exist."[27] The

---

_18/b3881046.htm?from=presignon&class=//www.businessweek.com/premium/content/04_18/b3881046.htm?se=1.

[22] Gillmor, *supra* note 12.

[23] Ryan Singel, *Gmail Still Sparking Debates*, WIRED, Apr. 24, 2004, *at* http://www.wired.com/news/infostructure/0,1377,63204,00.html.

[24] Council Directive 95/46/EC, art. 7(a), 1995 O.J. (L 281) 31.

[25] *A Move to Block Gmail Service*, WIRED, Apr. 13, 2004, *at* http://www.wired.com/news/business/0,1367,63041,00.html?tw=wn_story_related.

[26] *See id*. (describing that data protection laws give consumers right to their data, which includes deletion); Council Directive 95/46, art. 6(e), 1995 O.J. (L 281) 31, 40 (guaranteeing that personal data is "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"). Each E.U. nation implements guidelines, so to be compliant, Google will need to consider each nation's guidelines. This iBrief will consider the U.K. implementation as a model.

[27] Data Protection Act 1998 Legal Guidance, Information Commissioner, Version 1, at 3.5, *at* http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Data%20Protection%20Act%201998%20Legal%20Guidance.pdf. [hereinafter "Legal Guidance"].

U.K. Guidelines provide the data controller with a limited amount of discretion to make this evaluation.

¶10 Gmail's practice of backing up servers is standard in the webmail industry[28] and does not appear to violate the Directive. Gmail only stores information as long as necessary and is quite open about its backup procedures. Gmail's privacy policy acknowledges that it keeps "back-up copies of data for the purposes of recovery from errors or system failure," thus "residual copies of e-mail may remain on [Gmail's] systems for some time, even after [e-mail has been] deleted from [the user's] mailbox or after the termination of [the user's] account."[29] Accounts are deactivated two days after a user's request; however, residual copies of information may be left on the system for an extended period of time.[30] The extended data retention is necessary to protect users against server crashes and lost data. Nevertheless, Gmail makes "reasonable efforts to remove deleted information."[31] Eventually, the backup data on the offline tapes is erased.[32]

¶11 Gmail's server backup practices appear to be equal to, if not more compliant than its major competitors. When a user deletes his or her account from Yahoo! there is a 90-day lag before the account is deleted. The back-up storage data may not be deleted for even greater lengths of time.[33] When a Hotmail account is closed, the stored e-mail is permanently deleted; however, it is unclear when the backup e-mails are cleared from the system.[34]

C. Law Enforcement and the Electronic Communications Privacy Act

¶12 Another risk of increased data storage relates to its accessibility by law enforcement agencies. Under the Electronic Communications Privacy Act (ECPA),[35] a governmental entity must obtain a warrant to access the

---

[28] McCullagh, *supra* note 19.
[29] *Gmail Privacy Policy*, *supra* note 17.
[30] *Id.*
[31] *Id.*
[32] Gillmor, *supra* note 12.
[33] *Yahoo! Privacy Center: Data Storage*, YAHOO!, *at* http://privacy.yahoo.com/privacy/us/archives/details.html (last visited Oct. 9, 2004).
[34] *Close Accounts*, HOTMAIL, *at* http://www.hotmail.msn.com/cgi-bin/accountclose (last visited Oct. 29, 2004).
[35] Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (2000)). The ECPA includes Title I, the Wiretap Act, 18 U.S.C. §§ 2510-2522, and Title II, the Stored Communications Act, 18 U.S.C. §§ 2701-2711. *See* United States v. Councilman, 373 F.3d 197, 200 (1st Cir. 2004) (describing the ECPA).

content of e-mail stored for less than 180 days.[36] However, the governmental entity may access content of messages stored longer than 180 days through more relaxed standards.[37] As a result, users storing e-mail for long periods of time will have their communications more readily accessible to law enforcement agencies. Gmail's one gigabyte of storage space would increase this risk, particularly given that Google estimates one gigabyte could hold a decade worth of e-mail. [38] Yet this danger is not exclusive to Gmail. It exists with any e-mail service and is merely amplified by Gmail's storage capacity.[39]

¶13 Privacy organizations are not solely concerned with law enforcement agencies accessing data stored by consumers. They are also concerned about the data that is not immediately deleted by ISPs. Advocates worry law enforcement and other government agencies will take advantage of the Gmail infrastructure to search for users and subpoena information stored on the servers. This concern stems from the possibility that e-mail may not be instantaneously deleted, remaining accessible for long periods of time.[40]

¶14 In addition, privacy proponents warn that "law enforcement agencies may want to take advantage of the scanning to demand that Google – or other companies offering similar services – help them single out e-mail users based on the content of their correspondence."[41] This is not without precedent. In 2001, the Federal Bureau of Investigation compelled an "automobile navigation service to convert its system into a tool for monitoring in-car conversations."[42] Gmail has capabilities government monitoring and intelligence agencies have pursued in the past, namely Total Information Awareness and Carnivore.[43] Although Google does not utilize

---

[36] 18 U.S.C. § 2703(a) (2000).

[37] *Id.* § 2703(a) (e-mail stored for over 180 days may be available as stipulated under subsection (b) of this section); *Id.* § 2703(b) (a government entity may access e-mail content either through a warrant or a notice to the customer or subscriber in addition to either an administrative subpoena or a court order).

[38] Asaravala, *supra* note 7.

[39] Zetter, *supra* note 14.

[40] McCullagh, *supra* note 19.

[41] *Google Gets More Gmail Guff*, WIRED.COM, Apr. 7, 2004, *at* http://www.wired.com/news/business/0,1367,62976,00.html?tw=wn_tophead_6.

[42] Kevin Poulsen, *Court Limits In-Car FBI Spying*, REGISTER, Nov. 20, 2003, *at* http://www.theregister.co.uk/2003/11/20/court_limits_incar_fbi_spying/. However, though the company complied for 30 days, the company brought the case to federal court to block the order and eventually won in the United States Court of Appeals for the Ninth Circuit. *Id. See* Company v. United States, 349 F.3d 1132 (9th Cir. 2003).

[43] Hoffman, *supra* note 11. The purpose of Total Information Awareness was "to perform data analysis 'to determine links and patterns indicative of terrorist

this technology to collect information relating to specific users,[44] it would be feasible for law enforcement to seek a legal order compelling Gmail (or other webmail companies) to use its technology in this way. As has been noted, however, this is an issue that applies to many webmail services. Privacy advocates should refrain from attacking Gmail for implementing practices common to the e-mail industry. While Gmail may provide users with more storage space than other e-mail providers, its actions should not be the focus of privacy challenges. Advocates should concentrate on eliminating e-mail abuse by law enforcement agencies as opposed to demonizing Google for increasing its users' storage capacity.

III. ADSENSE: COMPLIANCE, REGULATION AND SOCIETAL EXPECTATIONS OF PRIVACY

¶15 Privacy advocates worry that Gmail's use of Adsense technology will further decrease societal expectations of privacy in electronic information.[45] They have also argued that Gmail's use of Adsense in e-mail violates various privacy laws and California is considering a bill that would outlaw the use of Adsense for e-mail advertising purposes.

A. Electronic Communications Privacy Act

¶16 Critics claim that Gmail's Adsense technology violates the ECPA.[46] The statute creates two criminal offenses. First, it prohibits *intentionally accessing* stored electronic communications without authorization.[47] Second, it precludes *intentionally intercepting* any wire, oral, or electronic communication.[48] Various appellate courts, including most recently the United States Court of Appeals for the First Circuit, have held that the intercept provision does not govern e-mails in electronic storage.[49] Since courts have recognized that Title I of the ECPA does not apply to "electronic communications," the e-mail in Gmail's servers would

---

activities.'" *Id.* Carnivore, an FBI tool, selects and records Internet traffic based on their content. *Id.*

[44] Paul Boutin, *Read My Mail, Please*, SLATE.MSN.COM, Apr. 15, 2004, *at* http://slate.msn.com/id/2098946/.

[45] Letter from Pam Dixon et al., Executive Director, World Privacy Forum, to Sergey Brin and Larry Page, Co-Founders, Google Inc. (Apr. 6, 2004), *at* http://www.privacyrights.org/ar/gmailletter.htm.

[46] Zetter, *supra* note 14.

[47] 18 U.S.C. § 2701(a) (2000).

[48] *Id.* § 2511.

[49] United States v. Councilman, 373 F.3d 197, 203-04 (1st Cir. 2004) (stating that electronic communications were not meant to be covered by the Wiretap Act). However, the opinion in the First Circuit was withdrawn and was heard en banc on December 8, 2004. United States v. Councilman, 385 F.3d 793, 793 (1st Cir. 2004).

not be covered. Title II would also not affect Gmail because it requires explicit unauthorized access,[50] something Gmail avoids by obtaining permission from users to access their accounts in its standard user agreement. Furthermore, the ECPA is inapplicable to Google because it provides an exception for entities providing the electronic communication service.[51]

B. California's Wiretapping Law

¶17 Some privacy organizations, including the Electronic Privacy Information Center (EPIC), accuse Gmail's Adsense technology of violating California's wiretapping law.[52] The statute makes it a crime to willfully and without the consent of *all* parties to a communication read or learn the contents or meaning of any message while it is in transit or received in the state.[53] EPIC argues that Gmail violates California's wiretap law by willfully reading e-mail messages without consent from the sender.54 Furthermore, EPIC believes scanning "e-mails for marketing placement constitutes an attempt to 'learn the contents or meaning' of the communication."[55]

¶18 Some lawyers in the field of surveillance-related law argue that EPIC's reading of the California statute is flawed.[56] The California penal code does not expressly define communication and one California court has held that the "provision covered only telegraph interception and telephone wiretapping, but not electronic communications such as E-mail."[57] Even if the statute applies to e-mail, Gmail only reads stored e-mail and would not meet the typical "in transit" definition of wiretap.[58] Further, it is arguable

---

[50] 18 U.S.C. § 2701(a).
[51] *Id.* at § 2701(c).
[52] Letter from Chris Jay Hoofnagle et al., Associate Director, EPIC, to Bill Lockyer, DOJ-OAG (May 3, 2004), *at* http://www.epic.org/privacy/gmail/agltr5.3.04.html.
[53] CAL. PENAL CODE § 631(a) (2004).
[54] Hoofnagle, *supra* note 52.
[55] *Id*.
[56] Declan McCullagh, *Does Gmail Break Wiretap Laws?*, CNET NEWS.COM, May 4, 2004, *at* http://news.com.com/2100-1038_3-5205554.html?tag=nefd.hed.
[57] Thomas R. Greenberg, *E-mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 238 n.102 (1994); Mark E. Schreiber, *Employer E-mail and Internet Risks, Policy Guidelines and Investigations*, 85 MASS. L. REV. 74, 86 (Fall 2000) (citing Flanagan v. Epson Am., Inc., No. BC007036, slip op. (Cal. Super. Ct. Jan. 4, 1991) which held that the wiretap statute did not apply to e-mail communications systems).
[58] McCullagh, *supra* note 56. For example, in one case in the early 1970's, a defendant relied on an answering service, which took the call and transcribed the

whether the process that matches advertisements to e-mail text falls under the "read" or "learn" requirement found in the statute;[59] if it does, then spam-filters used by other webmail services, which read e-mail text for content, would also violate this statute.

C. Fourth Amendment Expectations of Privacy

¶19 Gmail critics have also claimed that its practices conflict with the policies behind the Fourth Amendment and the "reasonable expectation of privacy."[60] Under Fourth Amendment jurisprudence, an individual has an expectation of privacy when the person's conduct "exhibits an actual (subjective) expectation of privacy," and that expectation "is one that society is prepared to recognize as reasonable."[61] In the context of e-mail, courts have held there to be a "limited reasonable expectation of privacy. . . . [e]-mail is almost equivalent to sending a letter via the mail."[62] "When an individual sends or mails letters, messages, or other information on the computer, that . . . expectation of privacy diminishes incrementally."[63] Once the e-mail message is received, the sender no longer has any expectation of privacy in its contents.[64]

¶20 Gmail will not have any substantial impact on e-mail users' expectations of privacy because it is offering services similar to those offered by its many competitors. The only major difference is that Gmail intends to employ its Adsense technology, while its competitors pursue other methods for generating advertising revenue. Yahoo!, for example, displays advertising banners from third-party ad servers on users' e-mail pages.[65] By consenting to Yahoo!'s privacy policy, a user gives consent to

---

message onto a piece of paper for the defendant to pick up. People v. Wilson, 94 Cal. Rptr. 923, 925 (Cal. Ct. App. 1971). The court determined that Section 631 did not apply because consent was given, but even if it did apply, the information was not obtained "while" the message was "in transit" but "after" it had passed "over" the telephone wire. *Wilson*, 94 Cal. Rptr. at 926.

[59] McCullagh, *supra* note 56 (stating that the "relatively dumb computer program" can't be said to "read" or "learn" text under California law's requirements).

[60] Templeton, *supra* note 6.

[61] Commonwealth v. Proetto, 771 A.2d 823, 830 (Pa. Super. Ct. 2001) (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

[62] *Id.* at 831 (quoting United States v. Charbonneau, 979 F.Supp. 1177, 1184 (S.D. Ohio 1997)).

[63] *Id.* (quoting United States v. Charbonneau, 979 F.Supp. 1177, 1184 (S.D. Ohio 1997).

[64] *Id.*

[65] *Yahoo! Privacy Center: Third Party and Affiliate Cookies on Yahoo!*¸ *at* http://privacy.yahoo.com/privacy/us/adservers/details.html (last visited Oct. 9, 2004).

allow these third-party affiliates to send cookies to the user's computer to track ad information. Opting out of this practice requires the user to individually opt-out of each ad partner, some of which do not even provide an opt-out option.[66]

¶21 Unlike Yahoo!, Gmail does not use advertising banners and its embedded Adsense advertisements do not place cookies on users' computers. Although Gmail uses cookies[67] to customize usage and record user data for internal business purposes,[68] Gmail's privacy standards are comparable with those of the industry.[69] The only minor deficiency is that Gmail does not bear the TRUSTe mark, but this should not single Gmail out for privacy criticism.[70] TRUSTe is simply a "seal of approval" that companies can pay to register and receive. While this seal may reassure the privacy neophyte, a savvier user will realize the protection is relatively minimal, as "TRUSTe does not prevent companies from collecting as much data as they want and trading it . . . . [They] simply require[] that companies disclose their actions."[71]

¶22 Given that Gmail's privacy provisions are on par with the rest of the webmail industry, arguments of a decreased collective expectation of privacy at the hands of Gmail are overstated. If critics are truly worried

---

[66] *Id.* Hotmail's policy is similar to Yahoo!'s. *MSN Privacy Statement*, MSN, *at* http://privacy.msn.com/ (last visited Oct. 9, 2004).

[67] Cookies are a form of communication between a server and a user. *HTTP Cookie*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/HTTP_cookie (last visited Oct. 9, 2004). It is typically used in HTTP transactions to "authenticate or identify a registered user of a web site" and "track[ ] a particular user's access to a site." *Id.*

[68] *Gmail Privacy Policy*, *supra* note 17.

[69] *Id.* The author asserts that this is true not only because Gmail believes so, but also because of the analysis done comparing the salient points in the privacy policies of Hotmail, Yahoo!, and Gmail done in this paper.

[70] TRUSTe was founded by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium and acts as an independent, nonprofit organization to certify the privacy self-regulation of Web sites. *TRUSTe's Mission*, TRUSTE, *at* http://www.truste.org/about/mission_statement.php (last visited Oct. 9, 2004).

[71] Carrie McLaren, *Privacy for Dummies? Corporations Hide Behind Fake Net Privacy Solutions*, STAY FREE! MAGAZINE, *at* http://www.stayfreemagazine.org/archives/15/privacy.html (last visited Apr. 9, 2005). If privacy advocates are truly sincere about raising concerns about Gmail's practices, then they should not hold back on denouncing the practices of Gmail's peers merely because they hold the "seal of approval" of a TRUSTe mark. In fact, a TRUSTe mark may be dangerous because it gives a web user a false sense of security when viewing the mark. *See id.* (describing how people will see the seal of approval and be reassured without realizing that these companies will still be able to collect data about them).

about a decreased expectation of privacy due to e-mail they would be better served addressing the entire industry as opposed to targeting a single actor.

D. California's Proposed Anti-Gmail Law

¶23 Concerns about Gmail's scanning techniques have led to proposed legislation in California targeting Gmail's e-mail scanning practice.[72] Originally drafted by State Senator Liz Figueroa (D-Fremont),[73] the amended proposal would forbid a webmail provider from divulging[74] or deriving[75] "personally identifiable information, user characteristics, or content of an electronic mail or instant message."[76] The proposed legislation provides exceptions allowing providers to divulge or derive information, so long as the information is not "for the provider's marketing purposes."[77] Thus, many useful technologies that scan e-mail content, such as spam filters, advertisement blockers, and virus scanners[78] would be excepted by the legislation.[79] In addition to regulating information usage, the legislation also requires providers to "delete an electronic communication when the customer has indicated he or she wants the communication deleted."[80]

¶24 The Gmail legislation has a narrow purpose, forbidding Gmail's Adsense scanning practice, while simultaneously allowing other industry

---

[72] *Fact Sheet for SB1822: Ban on Secretly Scrutinizing E-Mail Messages for Targeted Advertising*, *at* http://democrats.sen.ca.gov/senator/figueroa/ (last visited Oct. 10, 2004). For up to date information about the bill, visit http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_1822&sess=PREV&house=B&site=sen.

[73] To view Sen. Figueroa's webpage, visit http://democrats.sen.ca.gov/senator/figueroa/.

[74] "'Divulge' means to make personally identifiable information, user characteristics, or content of an electronic mail or instant message known to a person other than the addressee or intended recipient of the electronic mail or instant message." S.B. No. 1822, amended July 23, 2004, 1798.88(e).

[75] "Derive" means "to deduce or infer personally identifiable information, user characteristics, or content of an electronic mail or instant message." *Id.* 1798.88(d).

[76] *Id.* 1798.88.1(a); *Id.* 1798.88.2(a).

[77] *Id.* 1798.88.1(c); *Id.* 1798.88.2(b)(2).

[78] *Id.* § 1(c).

[79] *Id.* 1798.88.1; *Id.* 1798.88.2. Other uses that would fit the exception include audio content translation for the blind, and automatic message sorting and forwarding.

[80] *Id.* 1798.88.3(b). "Deletes an electronic communication" means "to take reasonable technical measures to ensure the electronic mail is inaccessible and unretrievable in the normal course of business." *Id.* 1798.88(c).

scanning practices targeting viruses and spam to continue.[81] Privacy advocates supporting the bill claim that the exceptions are justified because scanning for viruses and spam removes harm, whereas Gmail's Adsense scanning inserts "spam-like commercial advertising."[82] Furthermore, advocates worry that users may alter their behavior due to the surveillance created by the Adsense process.[83]

¶25 However, proponents of the legislation overlook that Adsense is not significantly different than many current advertising practices. Gmail's targeted advertisements are hardly different than receiving coupons from your local supermarket based on past purchases. Users willingly subject themselves to having their purchasing habits monitored and in return they receive discounts on those items. Similarly, Gmail users knowingly subject themselves to targeted e-mail advertisements, which in return subsidize the cost of two Gigabytes of webmail storage. Furthermore, attacking technology created for "marketing purposes" may have a detrimental effect on the online industry. Many Internet-based businesses rely on advertising as a predominant revenue model.[84] Eliminating this source of revenue will likely result in a less robust online environment. In addition, Adsense may ultimately increase the effectiveness of e-mail as an advertising medium, resulting in decreased reliance on intrusive e-mail messages, pop-up ads, and targeted banner ads.[85] Such a result would be positive for e-mail users. As one proponent of Gmail notes, having a tasteless pop-up ad at the bottom of an e-mail about a death in the family makes "Gmail's ad strategy sound[] appealing, not invasive."[86] Viewing the facts, the proposed California legislation is a dangerous overreaction. The bill would stop Adsense technology dead in its tracks before the actual effect of its implementation is known.

IV. POTENTIAL SOLUTIONS

¶26 Gmail is still in its beta testing period, giving Google an opportunity to implement internal changes to its product or policies before

---

[81] Wildstrom, *supra* note 21.
[82] Senator Liz Figueroa, *Fact Sheet for SB1822: Ban on Secretly Scrutinizing E-Mail Messages for Targeted Advertising* (on file with author).
[83] Templeton, *supra* note 6.
[84] *See* Catherine Yang & Jay Greene, *You've Got Mail—But Not Enough Ads*, BUSINESSWEEK, Oct. 25, 2004, at 48 (describing the importance of advertising and its effect on AOL's business strategy).
[85] *About Gmail*, *supra* note 3. To see an example of the textual ads, visit http://Gmail.google.com/Gmail/help/screen2.html. Gmail technology also filters advertisements that reflect "sensitive or inappropriate content." *Gmail and Privacy*, *supra* note 17.
[86] Boutin, *supra* note 44.

releasing it to the public.[87] In addition, Google is in a position to recommend industry-wide changes that would affect all webmail services. This section analyzes the benefits and detriments of several options that would improve webmail-user privacy.

A. User Opt-In for Advertising

¶27 One potential solution is to allow users to opt-in for Adsense advertising.[88] In an opt-in program, the user could use Gmail without the scanned ads, but would be given significantly less storage space.[89] While consumers may like the added choice, less storage space limits the effectiveness of Gmail's search and organization features.[90]

¶28 If Gmail were to offer a stripped-down version for users who opt-out of text-sensitive ad placement, then there may be little to distinguish Gmail from its webmail competitors. Furthermore, such an option would affect sales of context-sensitive ads. Since advertising sales are somewhat dependent on the amount of users that view the ads,[91] if a significant number of users do not opt-in, then the advertising space will be worthless. Ideally, an equilibrium could be reached whereby users would opt-in to provide Gmail profit on ad-sales and Gmail could set a price for premium service that would make up for lost ad revenues.

B. Sender Opt-Out

¶29 A second option is to allow e-mail senders an opt-out option that would prevent e-mails sent to a Gmail account from being scanned with Adsense technology. An opt-out option could be achieved by adapting the "Robots Exclusion Standard" to e-mail.[92] This standard is used by webmasters that do not want their websites to be searched.[93] These websites contain a "robots.txt" file that is read by search engines, like

---

[87] *Gmail and Privacy*, *supra* note 17.
[88] At present, Google does not plan to offer this option. Boutin, *supra* note 44.
[89] *Id*.
[90] Searching capabilities within the Gmail system is a large sell for Google. *About GMail*, GMAIL, *at* http://gmail.google.com/gmail/help/why_gmail.html (last visited Oct. 9, 2004).
[91] Google ad customers pay a base amount of $5 and then an additional amount of cost per click. *How Much Does AdWords Cost?*, GOOGLE, *at* https://adwords.google.com/support/bin/answer.py?answer=6382&hl=en_US (last visited Oct. 10, 2004). Thus, the less people who view the ads, the less people are able to click on ads.
[92] Boutin, *supra* note 44.
[93] *Id*.

Google, and results in the site's exclusion from search engine databases.[94] In the e-mail context, there could be an indicator attached to a sender's e-mail that prevents Gmail from scanning it.

¶30 Although technically feasible, its implementation would be difficult because it would require industry-wide standardization and a heightened level of knowledge by senders to attach the necessary tags. The standard would require Gmail to agree to adjust its system to look for a do-not-scan tag on e-mail and it would require other e-mail services to allow an attachment or tag in their e-mail system. Furthermore, there is no incentive for users not to opt-out, or for other webmail services to set this opt-out as its default setting; each would have a detrimental affect on Gmail advertising sales.

C. E-mail Encryption

¶31 Like most webmail services, Gmail does not send its e-mail in encrypted form; thus, while in transit, e-mail is as open to read as a postcard.[95] Gmail has had discussions with the Electronic Freedom Foundation about the possibility of encrypting its e-mail.[96] One potential example is Groove,[97] a virtual office software suite that allows users to send encrypted XML documents and messages to each other securely across the Internet.[98] Other standard encryption models include SMTP-over-TLS[99] or S/MIME[100] and PGP.[101] Adsense technology could still function in conjunction with encrypted e-mail and the encryption would alleviate concerns about access to law enforcement, as they would now need a

---

[94] *Robots.txt Tutorial*, SEARCH ENGINE WORLD, *at* http://www.searchengineworld.com/robots/robots_tutorial.htm (last visited Oct. 9, 2004).
[95] Templeton, *supra* note 6.
[96] Gillmor, *supra* note 12.
[97] *Id.*
[98] Kathleen Melymuka, *Sidebar: How Groove's Swarming Technology Works*, COMPUTERWORLD, July 28, 2003, *at* http://www.computerworld.com/managementtopics/management/story/0,10801,83407,00.html.
[99] Simple mail transport protocol over transport layer security. P. Hoffman, *RFC 3207 – SMTP Service Extension for Secure SMTP over Transport Layer Security*, Network Working Group, Feb. 2002, *at* http://www.faqs.org/rfcs/rfc3207.html.
[100] Secure / Multipurpose Internet Mail Extensions. *S/Mime*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/S/MIME (last visited Oct. 10, 2004).
[101] Templeton, *supra* note 6. PGP is Pretty Good Privacy and provides cryptographic privacy and authentication. *Pretty Good Privacy*, WIKIPEDIA, *at* http://en.wikipedia.org/wiki/PGP (last visited Oct. 10, 2004).

warrant to access a user's data instead of a mere subpoena.[102] Gmail already uses an SSL-encrypted login through a secure HTTPS link, which protects users from having their passwords stolen when they login.[103] Although e-mail encryption would add a layer of protection against access by third parties or law enforcement, encrypting Gmail messages[104] may prove costly and require "rearchitecting the whole back end" of the software.[105]

D. Improving Privacy Standards

¶32 Privacy and civil liberties groups want Gmail to clarify its privacy policies and how it will use the mined data.[106] While Google frequently states it will not infringe on their users' privacy rights, hackers or law enforcement agencies could potentially manipulate Gmail's technology. Furthermore, there is no guarantee that Gmail will not use its technology to violate users' privacy if it proves profitable in the future.

¶33 Google has stated that users will be notified on the Gmail login page when there are "any significant changes to [its privacy] policy."[107] Should users choose to eventually leave Gmail, they can take advantage of Gmail's POP (Post Office Protocol) support for its webmail service. POP allows users to access their e-mail offline, as well as download and backup their e-mail data.[108] Therefore, if Gmail's privacy policy changes to the point where users decide to close their accounts, the POP access allows them ample methods of keeping the information that has been stored on Gmail. However, Gmail should still strive to securely delete users' e-mail after closing an account; such a feature is currently available in Mac OS X

---

[102] Templeton, *supra* note 6.

[103] *Can I Access Gmail With a Secure HTTPS Link?*, GMAIL *at* http://gmail.google.com/support/bin/answer.py?answer=8155&query=encryption&topic=&type=f (last visited Oct. 10, 2004).

[104] Gmail does not offer any encryption support for PGP/GPG or any other encryption protocols. *How Can I Use PGP or GPG With Gmail?*, GMAIL *at* http://gmail.google.com/support/bin/answer.py?answer=10342&query=encryption&topic=&type=f (last visited Oct. 10, 2004).

[105] Gillmor, *supra* note 12.

[106] Dixon, *supra* note 45.

[107] *Gmail Privacy Policy*, *supra* note 17. Of course, Gmail has a feature whereby a user can click on a box at login which allows Gmail to store a cookie containing your username and password and completely bypass the Gmail page without logging in. *Id.* Presumably Gmail would disable this feature when a significant privacy changes is posted.

[108] *What is POP, and How Do I Use It?*, GMAIL, *at* http://gmail.google.com/support/bin/answer.py?answer=10350&ctx=match (last updated Feb. 16, 2005).

and PGP for Windows.[109] If users are free to change e-mail services when changes are made to privacy policies, then Gmail will have fulfilled its obligations to the consumer by providing the right to choose a webmail service based on its commitment to user privacy.

V. CONCLUSION

¶34 Privacy advocates should not target Gmail for practices that are widespread in the industry and legislators should not hastily enact laws to impede certain technologies. Gmail's use of Adsense has the potential to re-legitimize e-mail as a medium for advertising[110] and Gmail's search capabilities provide numerous benefits to users.[111]

¶35 While Google's company motto is "Do No Evil,"[112] Google is also a business. Gmail provides a service and in return should be allowed to display its ads based on trigger words in the text. Consumers frequently complain when they choose to give up a little privacy for free services,[113] but webmail is another way for Google to compete against search-engine portals like Yahoo! and MSN who also have their own web services. Gmail offered two gigabytes of storage at a time when its competitors were dramatically cutting back on free storage to squeeze more profits from their customers.[114] Since Gmail's introduction, rivals have followed suit by offering more free storage space.

¶36 Privacy groups should work with webmail services to set reasonable standards which all webmail services can follow. Privacy groups claim Gmail's technology architecture functions like a building – "that building may be used by many different owners, and its blueprint may be replicated in many other places."[115] However, if a building can be used

---

[109] McCullagh, *supra* note 19.
[110] *See* Yang & Greene, *supra* note 84 (describing the importance of advertising and its effect on AOL's business strategy).
[111] Asaravala, *supra* note 7.
[112] *10 Things the Google Ethics Committee Could Discuss*, BBC NEWS.COM, *at* http://news.bbc.co.uk/1/hi/magazine/3732475.stm (last updated May 20, 2004).
[113] For example, complaints were lodged against online newspapers who asked their readers to register with personal information. *Web Newspaper Registration Stirs Debate*, CNN.COM, June 14, 2004, *at* http://www.cnn.com/2004/TECH/internet/06/14/newspapers.online.ap/index.html. However, asking readers for personal information in exchange for free access to content they would otherwise have to pay for seems fair. *Id.*
[114] Alex Salkever, *Google Drops an E-Mail Bomb*, BUSINESSWEEK ONLINE, Apr. 1, 2004, *at* http://www.businessweek.com/technology/content/apr2004/tc2004041_5024_tc120.htm.
[115] Dixon, *supra* note 45.

for malicious reasons, we do not prohibit constructing the building, we prohibit the bad behavior. Only if the webmail community establishes clear standards and clearly delineates what is considered "bad behavior" will Gmail be able to redesign its architecture or privacy policy. Gmail is a useful service, and instead of accusing Gmail of privacy abuse, privacy groups should stop their abuse of Gmail.