Open Letter to Google Regarding Its Proposed Gmail Service

From:

World Privacy Forum
Privacy Rights Clearinghouse
and
Australian Privacy Foundation
Grayson Barber, Privacy Advocate
Roger Clarke, Privacy Researcher and Advocate (Australia)
Bits of Freedom (Netherlands)
British Columbia Civil Liberties Association (Canada)
Calegislation
CASPIAN
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumer Task Force for Automotive Issues
Electronic Privacy Information Center
Federación de Consumidores en Acción (FACUA) (Spain)
Foundation for Information Policy Research (United Kingdom)
Mari Frank, Esq., Author of Identity Theft Survival Kit
Simson L. Garfinkel, Author of Database Nation
Edward Hasbrouck, Author and Consumer Advocate
Massachusetts Consumer Assistance Council
Massachusetts Consumers' Coalition
National Association of Consumer Agency Administrators (NACAA)
National Consumers League
PrivacyActivism
Privacy International (United Kingdom)
Privacy Rights Now Coalition
Privacy Times
Private Citizen, Inc.
Privaterra (Canada)
Public Information Research, Inc.
Utility Consumers' Action Network

April 6, 2004

Sergey Brin, Co-Founder & President, Technology
Larry Page, Co-Founder & President, Products
Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Brin and Mr. Page:

Google's proposed Gmail service and the practices and policies of its business units raise significant and troubling questions.

First, Google has proposed scanning the text of all incoming emails for ad placement. The scanning of confidential email violates the implicit trust of an email service provider. Further, the unlimited period for data retention poses unnecessary risks of misuse.

Second, Google's overall data retention and correlation policies are problematic in their lack of clarity and broad scope. Google has not set specific, finite limits on how long it will retain user account, email, and transactional data. And Google has not set clear written policies about its data sharing between business units.

Third, the Gmail system sets potentially dangerous precedents and establishes reduced

expectations of privacy in email communications. These precedents may be adopted by other companies and governments and may persist long after Google is gone.

We urge you to suspend the Gmail service until the privacy issues are adequately addressed.

Email Scanning in Google's Proposed Gmail Service

The email text scanning infrastructure that Google has built is powerful and global in reach. Google has not created written policies to date that adequately protect consumers from the unintended consequences of building this structure. It is, in fact, arguable that no policy could adequately protect consumers from future abuses. The societal consequences of initiating a global infrastructure to continually monitor the communications of individuals are significant and far-reaching with immediate and long-term privacy implications.

Currently, individuals may have the understanding that Google's system is not that different in nature from scanning messages for spam, which is a common practice today. There is a fundamental difference, however. With Gmail, individuals' incoming emails will be scanned and seeded with ads. This will happen every time Gmail subscribers open their emails to re-read them, no matter how long they have been stored. Inserting new content from third party advertisers in incoming emails is fundamentally different than removing harmful viruses and unwanted spam.

Another potential misconception about the Gmail system is that the scanning will take place in isolation. The email is scanned, and ad text is delivered. But that is not the end of the story. The delivery of the ad text based on emails is a continual "on the fly" stream. This technology requires a substantial supply chain of directory structures, databases, logs, and a long memory. Auditing trails of the ad text are kept, and the data could be correlated with the data Google collects via its other business units such as its search site and its networking site, Orkut.

Google has countered criticism of Gmail by highlighting that a computer, not a human, will scan the content of the e-mail, thereby making the system less invasive. We think a computer system, with its greater storage, memory, and associative ability than a human's, could be just as invasive as a human listening to the communications, if not more so.

That the Gmail scanning and monitoring is being used for advertising right now is distracting, because it is a transient use. Scanning personal communications in the way Google is proposing is letting the proverbial genie out of the bottle. Today, Google wants to make a profit from selling ads. But tomorrow, another company may have completely different ideas about how to use such an infrastructure and the data it captures.

Google could -- tomorrow -- by choice or by court order, employ its scanning system for law enforcement purposes. We note that in one recent case, the Federal Bureau of Investigation obtained a court order compelling an automobile navigation service to convert its system into a tool for monitoring in-car conversations. How long will it be until law enforcement compels Google into a similar situation?

Google has been quick to state that it does not intend to correlate or share consumer data between its business units. But unless Google puts a consumer promise into its privacy policy that states it will never correlate the data, then Google is not putting its money where its mouth is. In a nation of laws, Google needs to make its promises in writing.

Gmail's Potential Conflict with International Law

The Gmail system may conflict with Europe's privacy laws, specifically, Directive 95/46/EC, also called the EU Privacy Directive. This directive states, among other things, that users' consent must be informed, specific, and unambiguous (pursuant to Article 7(a) of Dir. 95/46/EC).

As it has been proposed, and based on the current Gmail privacy policy, the consent of EU-based Gmail users cannot necessarily be considered informed, specific, and unambiguous in regards to the scanning, storage and further processing of their e-mails. The need for informed, specific, and unambiguous consent also applies to the potential linking of EU citizens' e-mails to their search histories. Additional issues with data retention may also exist under the EU Privacy Directive.

The Dangers of Lowered Privacy Expectations in the Email Medium

Ultimately, however, this discussion is not solely about Google. It is about the global tools Google is building, and the ways these tools and systems stand to alter how individuals perceive the sanctity of private communications in the electronic sphere. These perceptions and standards may persist long after Google as a company is gone.

Google needs to realize that many different companies and even governments can and likely will walk through the email scanning door once it is opened. As people become accustomed to the notion that email scanning for ad delivery is acceptable, "mission creep" is a real possibility. Other companies and governments may have very different ideas about data correlation than Google does, and may have different motivations for scanning the body of email messages. Google itself, in the absence of clear written promises and policies, may experience a change of course and choose to profit from its large stores of consumer data culled from private communications.

The lowered expectations of email privacy that Google's system has the potential to create is no small matter. Once an information architecture is built, it functions much like a building -- that building may be used by many different owners, and its blueprints may be replicated in many other places.

Google's technology is proprietary, but the precedents it sets are not.

Conclusion

We request the following of Google:

1. First, Google must suspend its implementation of scanning the full text of emails for determining ad placement.

2. Second, Google must clarify its information retention and data correlation policy amongst its business units, partners, and affiliates. This means that Google must set clear data retention and deletion dates and establish detailed written policies about data sharing and correlation amongst its business units and partners.

Respectfully submitted,

Pam Dixon, Executive Director
World Privacy Forum

Beth Givens, Director
Privacy Rights Clearinghouse

and the following individuals and organizations:

John Corker, Chair
Australian Privacy Foundation

Grayson Barber
Privacy Advocate

Maurice Wessling
Bits of Freedom (Netherlands)

Murray Mollard, Executive Director
B.C. Civil Liberties Association (Canada)

Dian Black
Calegislation

Katherine Albrecht, Ed.M., Founder and Director
CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering)

Roger Clarke (Australia)
Privacy Researcher, Advocate

Ken McEldowney, Executive Director
Consumer Action

Jean Ann Fox, Director of Consumer Protection
Consumer Federation of America

Richard Holober, Director
Consumer Federation of California

Will deHoo, Director
Consumer Task Force For Automotive Issues

Chris Hoofnagle, Associate Director
Electronic Privacy Information Center

Francisco Sanchez Legrán, President of FACUA
Federación de Consumidores en Acción (Spain)

Ian Brown
Foundation for Information Policy Research

Mari Frank, Esq.
Author of the Identity Theft Survival Kit

Simson L. Garfinkel
Author, Database Nation

Edward Hasbrouck
Author and Consumer Advocate

Paul Schrader, Executive Director
Massachusetts Consumer Assistance Council

Paul J. Schlaver, Chair
Massachusetts Consumers' Coalition

Kathleen Thuner, President
National Association of Consumer Agency Administrators (NACAA)

Linda Golodner, President
National Consumers League

Deborah Pierce, Executive Director
PrivacyActivism

Simon Davies
Privacy International (United Kingdom)

Remar Sutton, Co-Founder
Privacy Rights Now Coalition

Evan Hendricks
Privacy Times

Robert Bulmash, President
Private Citizen, Inc.

Robert Guerra, Managing Director
Privaterra (project of Computer Professionals for Social Responsibility) (Canada)

Daniel Brandt, President
Public Information Research, Inc.

Michael Shames, Executive Director
Utility Consumers' Action Network

###