



Oct. 8, 2009

Councilman Bernard C. Parks
Chairman
Budget and Finance Committee
Los Angeles City Council
200 North Spring St.
Los Angeles,
CA 90012

Dear Chairman Parks:

I'm writing to express further concern about the proposal to replace the city's email system with a "cloud computing" system provided by Google along with other cloud applications from the Internet giant. It appears that Google changes its story depending on its audience and I urge your committee to question Google's representatives closely about the company's apparently contradictory statements on such fundamental matters as computer security.

The difference in tone between Google's attempts to reassure potential users of its applications about security concerns and its explicit warnings of the applications' risks in communications aimed at shareholders required by federal law smacks of hypocrisy. In a promotional document titled "Introduction to Google" the Internet giant said:

"As maintaining user trust is core to our business, Google goes to great lengths to protect the data and intellectual property on servers that host user data. These facilities are protected around the clock and we have a dedicated security operations team who focuses specifically on maintaining the security of our environment."

A Google spokesman tried to reassure those raising valid security and privacy concerns about the proposed Los Angeles system with this statement made to CNET news service on July 21:

"Government agencies at all levels -- federal, state, and city -- are looking to cloud computing as way to advance innovation while decreasing costs. We agree that security is a very important consideration for any organization considering cloud computing, and we've been working very closely with the City of Los Angeles to address any questions and concerns government officials or citizens might have. Security is at the core of how we design Google Apps, and as the City of Los Angeles' evaluation report notes, the proposed cloud computing system is an improvement over the level of security currently in place. It also provides other benefits of cloud computing -- such as increased

innovation at reduced cost -- which are driving the city's request for a cloud solution to suit its IT needs."

Such talk would be reassuring were it not for the words coming from the other side of the corporate mouth. When Google is communicating with shareholders and must meet federal requirements for full disclosure, the tone is entirely different. The reassurances completely disappear and the risks are highlighted. Contrast the earlier statements to those in Google's federally mandated Form 10-Q for the Securities and Exchange Commission (<http://www.sec.gov/Archives/edgar/data/1288776/000119312509163845/d10q.htm>). In the document filed on Aug. 4., signed by Patrick Pichette Senior Vice President and Chief Financial Officer, Google said:

*"...[A]s nearly all of our products and services are web based, the amount of data we store for our users on our servers (including personal information) has been increasing. Any systems failure or compromise of our security that results in the release of our users' data could seriously limit the adoption of our products and services as well as harm our reputation and brand and, therefore, our business. **We may also need to expend significant resources to protect against security breaches. The risk that these types of events could seriously harm our business is likely to increase as we expand the number of web based products and services we offer as well as increase the number of countries where we operate.**" [Emphasis added, Page 50.]*

Or this:

*"Our business may be adversely affected by malicious applications that make changes to our users' computers and interfere with the Google experience. These applications have in the past attempted, and may in the future attempt, to change our users' internet experience, including hijacking queries to Google.com, altering or replacing Google search results, or otherwise interfering with our ability to connect with our users. The interference often occurs without disclosure to or consent from users, resulting in a negative experience that users may associate with Google. **These applications may be difficult or impossible to uninstall or disable, may reinstall themselves and may circumvent other applications' efforts to block or remove them.** In addition, we offer a number of products and services that our users download to their computers or that they rely on to store information and transmit information to others over the internet. **These products and services are subject to attack by viruses, worms, and other malicious software programs, which could jeopardize the security of information stored in a user's computer or in our computer systems and networks.** The ability to reach users and provide them with a superior experience is critical to our success. If our efforts to combat these malicious applications are unsuccessful, or if our products and services have actual or perceived vulnerabilities, our reputation may be harmed and our user traffic could decline, which would damage our business." [Emphasis added, Page 51]*

And then there is this:

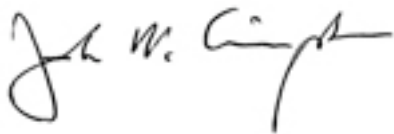
*"The availability of our products and services depends on the continuing operation of our information technology and communications systems. **Our systems are vulnerable to damage or interruption from earthquakes, terrorist attacks, floods, fires, power loss, telecommunications failures, computer viruses, computer denial of service attacks, or other attempts to harm our systems.** Some of our data centers are located in areas with a high risk of major earthquakes. Our data centers are also subject to break-ins, sabotage, and intentional acts of vandalism, and to potential disruptions if the operators of these facilities have financial difficulties. Some of our systems are not fully redundant, and our disaster recovery planning cannot account for all eventualities. The occurrence of a*

natural disaster, a decision to close a facility we are using without adequate notice for financial reasons, or other unanticipated problems at our data centers could result in lengthy interruptions in our service. In addition, our products and services are highly technical and complex and may contain errors or vulnerabilities. Any errors or vulnerabilities in our products and services, or damage to or failure of our systems could result in interruptions in our services, which could reduce our revenues and profits, and damage our brand." [Emphasis added, Page 52]

Google is attempting to reassure would-be purchasers of its services that there is nothing to worry about, while warning investors of everything that can go wrong so as to limit potential liability. Google wants to have it both ways. Maybe such hypocrisy is the norm in the world of corporate giants. However, you should demand a higher standard. I urge the Council's Budget and Finance Committee to demand precise explanations of Google's security and privacy guarantees.

If Google's system is adopted, the city must insist on adequate security guarantees. First, all data sent to Google's servers over the Internet should use SSL encryption through the https protocol. Data stored on Google servers must be encrypted and only the city should have the encryption key. Finally, to ensure that Google takes adequate security precautions, you should insist upon substantial financial penalties if security or privacy is breached.

Sincerely,

A handwritten signature in black ink, appearing to read "John M. Simpson". The signature is fluid and cursive, with a long horizontal stroke at the end.

John M. Simpson
Consumer Advocate

Cc: Greig Smith, Jose Huizar, Bill Rosendahl, Paul Koretz