09-1714

WORLD **PRIVACY** FORUM

July 16, 2009

The Honorable Antonio Villaraigosa
Mayor, City of Los Angeles
Room 303, City Hall
200 North Spring St.
Los Angeles, CA 90012

Re: Concerns about LA's proposed contract for migration of Los Angeles City email

Dear Mayor Villaraigosa:

We have concerns and questions about the proposed move of the City of Los Angeles' email and other services, such as word and other document processing, to a cloud-based computing system. If the City's proposed contract is approved, the City of Los Angeles will migrate to using Google Apps as its cloud service provider for email, as well as some of its day-to-day work with documents and other applications.

We are neither for nor against cloud computing. Our main concern is with the privacy implications of cloud computing. We believe that it is important that any individual or organization utilizing cloud computing be aware of the consequences of putting personal and other information in its possession in the cloud. There is considerable legal uncertainty about the status of data in a cloud computing environment – and this is a reason to proceed slowly and cautiously with a major contract like this.

The World Privacy Forum published a detailed analysis of the privacy and business implications of cloud computing services in February.[1] In this document, you will find a more complete discussion of some of the issues raised by cloud computing. In this letter, we hope to point out briefly some of the more troubling issues we have noted in the proposed contract.

---

[1] Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, World Privacy Forum, February 23, 2009. <http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf>.

I. Medical and health-related information

In the proposed contract, there is no mention or discussion of how emails and documents containing health data, medical data, employee medical data, insurance data, doctor-patient communications, AIDs data, genetic data, and other confidential or sensitive medical communications would be handled. If any of the City's agencies are health care providers subject to HIPAA, the sharing of patient information with a cloud provider requires, at a minimum, the use of a business associate agreement that complies with the HIPAA standards.

It is not clear that the City's proposed contract is adequate. More clear is that the obligation to meet HIPAA requirements was not mentioned anywhere in the contract. If our conclusion regarding HIPAA compliance is correct, using the facilities of the contract may place the City in violation of HIPAA, and patients may be exposed to privacy risks. Even where HIPAA does not apply, patient data is just as sensitive, and the risks to patients are the same.

II. Domestic Violence and Sexual Assault information

The proposed contract also does not mention how emails and documents containing information about domestic violence shelters or victims of domestic violence and sexual assault will be handled or managed. The contract does not mention how the City or its contractor will comply with the Violence Against Women Act (VAWA) and its confidentiality requirements regarding processing of any data regarding victims of domestic violence, sexual assault, and other covered issues.

The VAWA provisions impose some of the most stringent privacy protections of any law, and even the sharing of domestic violence information with contractors may violate the law. Regardless, the sharing of information on victims of domestic violence with a contractor may expose those victims to great harm.

III. Substance Abuse Information

Another federal law that may apply to some City programs regulates the confidentiality of clients of drug and alcohol abuse programs. The rules, found at 42 CFR Part 2, impose strict limits on use and disclosure of client information. California law also imposes confidentiality limits on the same records. The sharing of information on substance abuse patients with a contractor may violate these laws and may expose patients to harm. We find nothing in the contract that mentions the special privacy rules applicable to these records.

IV. Sensitive Information in General

Sensitive information about undercover police, people who are under police investigation, informants, and others is normally held very closely within the agencies that create the information. The sharing of this information with any third party may

present a threat to the individuals and to the functioning of law enforcement operations. We observe that the contract has some provisions addressing the special needs of these categories of information. We have no opinion whether the provisions are adequate.

However, we note that the City maintains considerable amounts of sensitive information other than for law enforcement purposes. We have already identified some privacy-sensitive information elsewhere in this letter. Additional information that is sensitive includes:

- Budget information (e.g., preliminary and unreleased budget information),
- Financing plans (e.g., plans for the sale of bonds),
- Appraisal documents (e.g., for property that the City is contemplating acquiring or selling),
- Contracting information (including trade secrets and other confidential information obtained from private businesses),
- Construction plans (e.g., routes under consideration for building a new highway),
- Negotiation documents for employment contracts with City workers and for other negotiations,
- Tax information, and more.

The contract's provisions for protecting data related to law enforcement records may or may not be adequate. The provisions in the contract about data related to various other categories of information that City residents or other City departments would consider to be sensitive are certainly inadequate.

We also wonder whether the sharing of advice from the City's lawyers would result in the loss of any available attorney-client privilege. We are not aware of any case law on this point, but the risk of losing protection for legal advice could potentially be significantly detrimental to the City.

V. Classified data

Various departments of the City may have information that has been classified for national security purposes by the federal government, designated as sensitive in other ways by the federal government or state government, or otherwise subject to court orders or other restrictions that require strict controls on use and disclosure. Only those with proper clearance or with a need to know may be allowed to see the information.

The transfer of any of this information under the contract may violate state or federal law, endanger national security, or result in harm to other important interests. The contract does not address the disparate requirements of these classes of information.

VI. Security

Different types of information may have different security requirements. For example, health information subject to the federal health privacy and security rules under HIPAA are subject to a specific set of security standards. Information classified by the federal

government for national security is subject to a different set of security standards. Tax information obtained from the Internal Revenue Service or from the State is subject to its own security rules. Other categories of information may have their own requirements. It is not clear that the security provided under the contract can meet all existing security obligations. The encryption contemplated by the contract may not meet all applicable encryption standards.

VII. Location

The contract (page 45) allows Google to store City data in any other country where the company maintains facilities.[2] City data could become subject to the laws of these countries by virtue its being processed by Google. Sensitive data about the City or its citizens could be subject to civil process in these countries, for example, to search and seizure under laws that are much less stringent than would apply if the information were maintained in California, or to other law enforcement access.

VIII. Ownership

The contract provides that the City "shall be entitled to an export of City Data…upon termination of the contract." That is an extraordinary provision. The contract does not require the contractor to delete the data upon contract termination. Its only obligation is to give a copy to the City. That suggests that the contractor could maintain a copy of the data. Why the contract would not require the contractor to eliminate all data from its possession at the termination of the contract is unclear.

IX. Solutions

There are a number of potential solutions to the problems and challenges posed by the proposed contract.

- First, the City needs to confer with all stakeholders in an open, transparent, and fair public comment process. This is not a contract that should be rushed into.

- Second, because the City maintains so much personal and business data of third parties, the City may wish to consider making its residents and businesses third party beneficiaries of the contract. In the event that the contractor uses or discloses information in violation of the security or confidentiality requirements of the contract, the party who has been harmed by the use or disclosure should be able to sue the contractor for damages. This would limit the City's liability and impose liability on the contractor where it belongs.

[2] See contract appendix 1.7, Data Transfer: "As part of providing the Service, Google may store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data."

- Third, the City should submit any new provisions it has incorporated for a second round of public comment, including the entire contract, so that the process is transparent for residents.

- Fourth, the City should conduct a formal independent risk assessment of the privacy, security, and confidentiality issues the contract raises. There is data that the City may choose to omit from cloud services altogether. Other data may be fine to put in the cloud. A risk assessment focused on this issue will assist the City in clarifying the problems before harm occurs.

X. Conclusion

We want to be clear that our main interest is in the privacy impacts this proposed contract presents, but the City has other confidentiality interests that it must protect. As we state in our report on cloud computing privacy, these issues are part and parcel of the legal ambiguities of cloud services, and need careful vetting and consideration regardless of which company may be providing the services. We have only had an opportunity to undertake a preliminary review of the proposed contract, and we have identified quite a few serious and unanswered issues.

Our concern is that the transfer of so many City records to a cloud computing provider may threaten the privacy rights of City residents, undermine the security of other sensitive information, violate both state and federal laws, and potentially damage vital City legal and other interests.

We believe that the City of Los Angeles has rushed into this without enough careful consideration of all of the consequences, and without enough attention to the details of protecting the privacy of the data contractually. We urge the City of Los Angeles to conduct a thorough analysis and risk assessment of all privacy and other confidentiality impacts that may occur, and we urge the City to protect its residents and itself from the many potential unintended consequences. We also reiterate that this contract be subject to several rounds of public comment so that the public and others can help the City to identify all the risks and concerns that the contract affects.

Sincerely,

/s/

Pam Dixon
Executive Director,
World Privacy Forum