CITY AND COUNTY OF SAN FRANCISCO

DEPARTMENT OF TELECOMMUNICATIONS AND INFORMATION SERVICES

Chris Vein
Executive Director

Telephone: (415) 554-0801

Ron Vinson
Chief Administrative Officer

Telephone: (415) 554-0803 Fax: (415) 554-4733

May 31, 2007

Ms. Nicole A. Ozer
Technology and Civil Liberties Policy Director
American Civil Liberties Union of Northern California
111 North Market Street, Suite 940
San Jose, California 95113

Dear Ms. Ozer:

This letter responds to the American Civil Liberties Union ("ACLU") comments about subscriber privacy provisions included in the wireless broadband network agreement between the City and County of San Francisco ("City") and EarthLink, Inc. ("Agreement"). Specifically, we respond to the public testimony of ACLU attorney Nicole Ozer made at the City's Board of Supervisor's Budget and Finance Committee hearing on May 14, 2007, and to ACLU's written comments included in a letter to the Board dated February 6, 2007.

We applaud the ACLU's efforts to ensure that the Agreement adequately protects the privacy and civil liberties rights of San Franciscans. However, we respond to specific ACLU comments, outlined below, which include inaccurate statements and omissions regarding the scope of privacy protections provided by the Agreement.

According to the Electronic Frontier Foundation ("EFF"), a leading Internet civil liberties and privacy advocate, "best practices" in online privacy protection requires a balancing between the legal and operational needs of the service provider and the need to protect the user's privacy and civil liberties.[1] Service providers must collect and use personal information for a variety of reasons, from billing and collections, to promotion and delivery of new services, to protecting the security and integrity of the network and the safety of other users.

Both the City and EarthLink strongly believe that protection of an individual's personal privacy is of paramount importance. EarthLink has a long and distinguished track record in fighting for the rights of its subscribers to remain anonymous and to safeguard their protected personal information ("PPI") from unauthorized use or disclosure. The City and EarthLink have worked long and hard to develop provisions in this Agreement that afford a high level of consumer privacy protection.

[1] See EFF, "Best Data Practices for Online Service Providers from the Electronic Frontier Foundation," (Aug. 19, 2004) p. 1 (available online at http://www.eff.org/osp/20040819_OSPBestPractices.pdf).

I. ACLU's Public Comments of May 14, 2007

First, we respond to Ms. Ozer's May 14th statement that the City's Agreement is less protective of personal privacy than wireless agreements in other cities, specifically Portland and Philadelphia. We respectfully disagree. This Agreement includes some of the most stringent privacy protections negotiated in a municipal wireless agreement, including the following significant requirements not found in other similar agreements.

1. Restrictions on "Location Information."

The Agreement contains ground-breaking restrictions on the use and retention of a specialized type of information, known as "location information." This information, unique to wireless services, can be linked with other PPI to reveal the physical locations of individual users. The Agreement allows users of EarthLink's fee service to opt out of all uses of location information (with specified exceptions), and requires EarthLink to delete location information after 60 days unless kept in aggregate (non-identifying) form, or retention is required by law, court order or an internal investigation to detect fraud, crime or a security breach of a material mature.

Neither the Portland nor Philadelphia agreements place any express restrictions on location information.

2. Reasonable prior notice required before disclosure in civil proceedings.

The Agreement protects the right of both "no fee" and "fee" service users to remain anonymous by requiring reasonable notice prior to disclosure of PPI in civil proceedings. Civil subpoenas served on an ISP demanding subscriber information are usually aimed at uncovering the identities of people who are posting anonymous comments.[2] Sometimes these demands are simply used in an attempt to stifle the speaker, without any sound legal basis or intent to follow through with the legal process.

Requiring EarthLink to provide the anonymous online speaker with notice of the subpoena before disclosing the information gives the speaker an opportunity to object to the disclosure (by filing a motion to "quash" the subpoena), and thus maintain his or her anonymity. Several states have considered legislation to require prior notice in these situations.[3] However, neither Portland nor Philadelphia require this important speech protection.

3. Restrictions on disclosure of personal information for criminal investigation or investigation related to national security.

Users of both the "fee" and "no fee" services will benefit from various restrictions on disclosure of PPI for national security and law enforcement purposes, including a requirement that EarthLink, if allowed by law, must require evidence of a court order before it may disclose PPI as part of a criminal investigation or investigation relating

---

[2] EFF, "Best Data Practices," p. 3.

[3] In 2003, California Assembly Member Joe Simitian introduced legislation to require that online consumers be notified before their personal identities are disclosed by their ISP as a result of a civil subpoena (AB 1143). The bill was passed by the California Assembly, but failed in the Senate. The City's Agreement effectively imposes the same protections that were contemplated in that legislation.

to national security, unless the disclosure is necessary to prevent fraud, protect network security, or protect property rights or safety of other users. The joint goal of the City and EarthLink is to prevent, to the extent legally possible, PII from being scrutinized as part of any unauthorized "fishing expeditions" by government or law enforcement officials sifting through EarthLink's records.

Neither the Portland nor Philadelphia agreements specifically require evidence of a court order prior to disclosing PPI to government officials or law enforcement.

4. Opt in provision for information sharing; opt out provisions for receiving marketing messages.

The Agreement provides that EarthLink may not share PPI collected from its fee service subscribers without the voluntary, affirmative consent of the subscriber, subject to certain exceptions. When PPI is shared with other entities as allowed under those exceptions, users may opt out of marketing communications from those entities. Although this provision might be viewed as slightly less restrictive than the Portland agreement (which requires an opt in for third party marketing communications), it is much more restrictive of PPI sharing than the Philadelphia agreement, which merely requires EarthLink to comply with its self-imposed, corporate privacy policy.

Responses to other comments made by Ms. Ozer are incorporated into the following response to ACLU's February 6, 2007 letter.

II. ACLU's Letter Dated February 6, 2007

With respect to the analysis of the Agreement presented by the ACLU in the above-referenced letter, we have the following point-by-point observations and suggestions for revising the "color coding" grades for the ACLU's four key principles:

ACLU Principle 1. The service should collect the minimum amount of personal information and maintain user records only so long as operationally necessary.

"What personal information is collected about users?"

The ACLU's recommendation is that, if possible, no personal information should be collected from its users. As discussed above, it is simply not feasible to operate a wireless broadband service without collecting and maintaining certain personally identifying information.

For the no fee service, the Agreement provides that only minimal information will be collected for login. This is possible because detailed personal information for billing and account services is not necessary. Therefore, little, if any, personal information will be collected. This box should therefore be colored green.

In the case of EarthLink's fee service, users will provide some personal information to establish an account, receive services, complete billing processes and get information about new services. In addition, certain information is required to comply with legal standards, protect against harm from criminal activity, security breaches and to protect the rights of other users. For example, EarthLink may need to retain certain location and

subscriber information to circumvent efforts by a user to distribute a computer virus or to identify and deny access to repeat copyright infringers.[4]

The Agreement balances these operational needs by creating a series of restrictions on information designated as "Protected Personal Information" (PPI). PPI may not be shared by EarthLink without the voluntary, affirmative consent of the user, subject to certain exceptions. Disclosure of PPI to law enforcement and in civil proceedings is subject to various other restrictions, described in detail above. Additionally, users may opt out of any use of location information, as described above. These restrictions are not acknowledged in the ACLU analysis.

"Are mechanisms available to allow users to opt in or opt out of any service that collects, stores or profiles information on the searches performed, websites visited, emails sent or any other use of the network."

The services provided pursuant to this agreement will enable users to access a vast number of third-party services that may collect PII. It is unreasonable to expect this Agreement to regulate PII practices of such unaffiliated services. Likewise, it is unrealistic to attempt to use this Agreement to impose changes to the PII collection practices of unrelated services (such as search engine services) provided by unaffiliated or affiliated service providers.

With respect to services provided by EarthLink under this Agreement, ACLU's analysis suggests that there are no provisions in the Agreement that apply to information collected regarding the activities of users of services on the system. However, with respect to EarthLink's fee service, the Agreement defines PPI to include any "Unique Information," if that information is associated with PPI (and thus identified as the activities of an individual user). Thus, if activity usage logs are associated with PPI, all of the privacy protections applicable to PPI described above (including the opt in and opt out provisions) also apply to these usage logs. If these logs are not associated with PPI (e.g., they are compiled as aggregate data) then they may be maintained without risk of harm to privacy of the users.

Moreover, one specific type of unique information, Location Information, receives more stringent protection in the Agreement. Users may opt out of any use of location information, but this protection is not acknowledged in the analysis.

"Are mechanisms available to allow users to opt in or opt out of any service that tracks information about the user's physical location?"

We fail to understand why this box is not solid green. The Network Agreement includes ground-breaking provisions limiting the uses of Location Information. This is provision specifically limits the length of time such information resides on the system to 60 days and allows users to opt out of any use of the information. The limited exceptions to these requirements have no negative effects on user's privacy. Neither the Portland nor Philadelphia wireless agreements include specific provision related to the unique privacy concerns raised by the collection of location information.

---

[4] The Digital Millennium Copyright Act provides that an Internet service provider, if it otherwise qualifies under the statute, is immune from liability for a third-party user's infringement as long as it has a policy of terminating repeat infringers (17 USC §§ 512(a); 512(i)(1)(A).

"How long is this information stored?"

We are unclear about what types of information "this" refers to. If it refers back to the preceding question, this box should be green, because EarthLink must delete Location Information after 60 days.

If "this" refers to all PPI, then we do not understand ACLU's recommendation that that data should "never" be retained for more than a few weeks. According to the EFF's "Best Data Practices," different types of personal information may need to be kept for different time periods, depending on operational needs of the service. For example, certain billing and collections information must be retained for as long as the user remains a subscriber of the system. As described above, session information may require retention for several weeks for operational or security reasons. Information that has been aggregated and is no longer linked to individual PPI may be kept for longer periods because there is no privacy risk.

Rather than negotiate complicated schedules for data retention, we allow EarthLink the discretion to craft data retention schedules to meet its own operational needs. We focused the privacy protections in this Agreement to address disclosure of PPI, especially disclosure to government and law enforcement agencies and disclosure in civil proceedings, where substantial harm to civil liberties and First Amendment rights are most likely to occur.

ACLU Principle 2. The service should not track user activities from session to session.

"Is information correlated to a specific user, device or location?"

ACLU's analysis faults the City's agreement with EarthLink because "Login information is required for access." We fail to see the harm of requiring the collection of minimal information for login purposes. Such information is necessary to operate the system, maintain billing processes, protect system security and integrity and protect other users from harmful acts. As explained above, we chose to focus the privacy protections in this Agreement to limit disclosure of PPI, especially disclosure to government and law enforcement agencies and disclosure in civil proceedings, where harm to civil liberties and First Amendment Rights are most likely to occur.

With respect to the "no fee" service, only minimal information will be collected for log in. This is possible because detailed personal information for billing and account services is not necessary. Therefore, little, if any, personal information will be collected, and any tracking of user activities will not likely be associated with PPI.

"Are users enumerated or assigned any unique number that can be used to track them from session to session?"

Again, this information may be operationally necessary for billing, system security and to protect users from harm. To the extent any unique identifier may be associated with an individual's PPI, it will be subject to the disclosure limitations described above.

ACLU Principle 3. The service should only use data for operation of the network and should not commercialize data without the voluntary, opt in consent.

"How is this information used?"

The ACLU analysis states that there is no limitation in the Agreement about how EarthLink may use PII. However, as discussed above, several limitations are placed on PII collected by the fee service, including "opt in" consent for disclosure to non-affiliates, "opt out" for use of location information and time limits for the retention of location information.

"Is information sold, traded or used for target advertising?"

ACLU's analysis of this question is inaccurate and misleading. For the fee service, Section 10.3.1.1 of the Agreement clearly states that "EarthLink will not share Protected Personal Information with any person or entity without the voluntary, affirmative consent of the user . . ." (subject to certain exceptions). This is an "opt in" requirement, and precisely meets the ACLU's recommendation for this question.

When PPI is disclosed under a specified exception, the user may opt out of receiving any marketing communications. These provisions are set forth in detail under the following principle, but are also applicable to this question.

With regard to the no fee service, little, if any, PPI will be collected for login. Thus the ability to develop targeted advertising lists will be minimized.

Both of these boxes should be shaded green.

ACLU Principle 4. The service should only disclose the personal information of users when it is truly legally necessary and give notice to users about disclosures as quickly as possible.

"When is information shared with third parties?"

ACLU comments that for EarthLink's fee service, there is no opt out for information sharing "to process payments, collection, order fulfillment, and service delivery." We note that users would be highly unlikely to opt out of information sharing that makes it possible to receive ordered products and services, and no best practices policies we found recommended an opt out option for payment processing and collections.

Both of these boxes should be shaded green.

"Are policies in place to respond to legal demands for users' personal information?"

We do not understand why these boxes are not both bright green, as the provisions set forth in this section are highly protective of individual users' privacy and First Amendment rights. The threat of government intrusion into anonymous online communications poses a significant threat of chilling free speech. This Agreement requires evidence of a court order prior to disclosure for law enforcement and national security investigations when allowed by law. The joint goal of the City and EarthLink is to prevent, to extent legally possible, PII from being identified as part of any unauthorized "fishing expeditions" by law enforcement officials sifting through EarthLink's records.

More importantly, EarthLink must provide reasonable prior notice to a user before disclosing PPI in response to a civil legal demand. This notice is critical in protecting the First Amendment right of online speakers to maintain their anonymity in the wake of frivolous lawsuits to force disclosure of the identity the speaker merely because the speaker's views may be unfavorable to others. Several states have considered legislation to require prior notice in these situations.[5]

All of these protections apply to both the fee and no fee tiers of service. As stated above, neither Portland nor Philadelphia have included these types of protections against unauthorized disclosure to law enforcement or in civil proceedings, even though such safeguards are essential to protect civil liberties and free speech rights of users.

III. Conclusion

In closing, we would question the wisdom of imposing stringent privacy protections only on those providers seeking to enter into municipal wireless agreements. If specific privacy concerns need to be addressed, they should be undertaken on an industry-wide basis, by amending applicable law. EarthLink has agreed to comply with all applicable laws related to privacy protection, including those enacted subsequent to execution of the agreement. Imposing more stringent privacy restrictions only on municipal wireless providers would create a competitive disadvantage for such providers, making such a venture (whether municipally owned or a public/private partnership) less likely to succeed in the marketplace.

If you have any questions or wish to discuss these matters further, please feel free to contact me.

Sincerely,

Barry Fraser
Policy Analyst

cc: Mayor's Office
Board of Supervisors
Ms. Susan Leal - PUC

[5] See the discussion on p. 2, preceding footnote 3.