

PRIVACY AGREEMENT TERMS AND CONDITIONS¹

I. TYPES AND SCOPE OF USER INFORMATION COLLECTED

A. Definitions

“**User**” means a person or entity connecting to the Internet through the Metro Connect Wireless Silicon Valley wireless network.

B. Registration Information

Metro Connect shall register each User, and create a **User Registration Profile**, which shall include the following information: Username, Password, and enough personal information to associate each Username with a known individual.²

¹ The Model Terms and Conditions are provided by law faculty and law students of Santa Clara University. They are provided in response to a request by Wireless Silicon Valley for a document responsive to the concerns voiced by participants in the public forum entitled Privacy and Security in a Wireless World held at Santa Clara University on August 23, 2006. See <http://www.jointventure.org/programs-initiatives/smartvalley/projects/wirelessv/PrivacyandSecurity.html>.

The Model Terms and Conditions are based on the following understandings. First, subject to completion of successful negotiations between the parties, Metro Connect through its partner Azulstar would be the network provider for the “Wireless Silicon Valley Network” spanning Santa Clara and San Mateo counties and other jurisdictions. Second, that Azulstar as network provider would serve as the interface between all network Users and the Internet. Third, regardless of whether Users opted for the free or pay tiers of service, all Users would be provided all of the privacy protections afforded by the Terms and Conditions and the Privacy Policy. Fourth, Wireless Silicon Valley would negotiate with the Metro Connect team to assure that the privacy protections afforded by the Terms and Conditions and the Privacy Agreement, if adopted, would be extended to all the Users in each of the forty-two jurisdictions.

Numerous requests were made to Metro Connect and Wireless Silicon Valley for information concerning proposed tiers of service, the anticipated availability of security protections based on service tiers, as well as samples of relevant privacy language contained in policies of Metro Connect partners. That information was not provided and hence is not incorporated in the documents.

It is anticipated and intended that this document will be merged with and harmonized with the sister document prepared by the law faculty and students of Stanford University entitled “Proposed Privacy Policy”.

² Law enforcement requires some way of attaching a username to a known individual. Ideally, the provider would be required to verify that an individual signing up for an account really is who he says he is. The policy behind this: an open network would be a playground for crackers who want to anonymously break into networked computers. Usually, these crackers leave only an IP address to trace. If an IP address is not capable of pointing to a specific individual at a specific time, then law enforcement will be unable to help victims of these computer crimes and bring the cracker to justice.

C. Service Information

After each user is registered, Metro Connect shall create a **User Service Profile**, which shall include the following information: username, the date and time the user connects to and disconnects from the network, and the IP address the network assigns to the user device. If the user has a metered account, Metro Connect may also keep a tally of the amount of data the user sends and receives over the network. Although the location of the particular network tower used to access the network may be used to provide location-focused advertising, location information shall never be logged.

In addition, Metro Connect may collect service related data necessary to assist with network support, operations, billing and performance monitoring. Service related data that connects an IP address with a specific known individual may also be collected.

D. Usage Information

Anonymous Individualized Profiles may be created to provide targeted advertising but must be stored in a separate database from registration and service information and service related data. An Anonymous Individualized Profile should only contain browsing history and any calculations or generated data done by the ad serving company that tells what ad to deliver next. It should not contain IP address information.

Metro Connect is not responsible for third party use or retention of user information obtained by accessing third party sites via the network. The user is solely and fully responsible for the use and transmission of any data to or from third party sites while using the network to access third party sites.

II. CONSTRAINTS ON ACCESS TO AND USE OF INFORMATION BY PROVIDER

A. Registration Information

User Registration Profiles, containing the information Metro Connect obtains about users during registration, will not be used for advertising purposes³ and will be kept separate from any information used for advertising. This information will be held as confidential and will not be sold, bargained for, traded away, or otherwise provided to any third party unless: (1) the user agrees to or requests such a transfer by expressly electing to opt in or (2) disclosure is required to comply with duly authorized local, state, or federal subpoenas, warrants or court orders. In addition, Metro Connect shall provide the User with a clear description of the information to be collected and how the information will be used prior to requesting User's consent to the transfer or disclosure of the information unless precluded from doing so by law.

³ Access to private information by a government-sponsored service provider is not uncommon. However, if identifying information were to be used for advertising, the ACLU would argue that a constitutional right to privacy (that cannot be sold, traded, or bargained away to the government) has been violated. The trade would presumably be privacy for internet access. This is particularly troubling when one considers those users who cannot afford broadband access because it raises the question of how much privacy a person can afford.

Metro Connect may also disclose User information to facilitate the investigation of breaches of Metro Connect's network terms and conditions of service, to protect the network against fraud or other abuse, or to enforce sanctions for such fraud or abuse. Metro Connect shall define the types of user behaviors that constitute fraud or abuse and shall provide prior express notice to all network users at time of contract for service.

B. Service Information

User Service Profiles, containing service information and service related data: (1) will not be used for advertising purposes, and (2) will be stored in separate logical and physical locations from any information used for advertising.⁴

This information will be held as confidential and will not be sold, bargained for, traded away, or otherwise provided to any third party unless: (1) the user agrees to or requests such a transfer by expressly electing to opt in or (2) disclosure is required to comply with duly authorized local, state, or federal subpoenas, warrants or court orders. In addition, Metro Connect shall provide User with a clear description of the information being collected and how the information will be used prior to requesting User's consent to the transfer or disclosure unless precluded from doing so by law.

Metro Connect may also disclose this information to facilitate the investigation of breaches of Metro Connect's network terms and conditions of service, to protect the network against fraud or other abuse, or to enforce sanctions for such fraud or abuse. Metro Connect shall define the types of user behaviors that constitute fraud or abuse and shall provide prior express notice to all network users at time of contract for service.

C. Metro Connect Employee Access to Information

Metro Connect may provide its employees, contractors and agents access to customer registration, service, usage or location information in the course of operating, developing and improving its services. Metro Connect shall contractually bind its employees, contractors and agents to use the information only as needed for the performance of the specific services related

⁴ The ACLU does not seem to be bothered by the use of anonymous profile data for advertising purposes, as long as no entity has the ability to link the profile to an individual. The compromise is to limit the use of user data obtained for registration purposes to administrative requirements and law enforcement operations. This strikes a balance that holds users accountable for using the network to break the law, while protecting the privacy of a user's web surfing habits.

In the spirit of striking this balance, registration and other information such as quality of service (which may be indicative of financial status) should be stored separately from any advertising related information. There should be no identifier that allows these two datasets to be combined. This would create a database of surfing habits of known individuals.

task. Employee failure to adhere to the required restricted use shall result in disciplinary action including but not limited to termination and/or criminal prosecution when applicable.⁵

D. Compliance with Applicable Statutes and Regulations

Metro Connect, including its affiliates and third parties with which it has contracts or subcontracts, agrees that it will comply with all applicable and relevant federal and California statutes and regulations, including, but not limited to, the following:

- a. Federal Law
 - i. 47 U.S.C. § 222: Privacy of customer information⁶
 - ii. 15 U.S.C. § 6501: Children’s Online Privacy Protection Act (COPPA), codified at 16 C.F.R. §§312.1-312.12.⁷
 - iii. Communications Assistance for Law Enforcement Act (CALEA)⁸
 - iv. The Electronic Communications Privacy Act (ECPA)⁹
 - v. Uniting and Strengthening America by Providing Appropriate Tools to Interrupt and Obstruct Terrorism (USA PATRIOT ACT), (PL 107-156, 2001 HR 3162)¹⁰

⁵ This provision is intended to deter Metro Connect’s employees from providing data brokers and others unauthorized access and/or illegal access to user information.

⁶ 47 U.S.C. §222- Privacy of customer information. This law defines and governs the ability of telecommunications providers to provide “customer proprietary network information” to third parties. It makes a distinction between such data, which generally cannot be provided to third parties without the customer’s permission, and aggregated data, which is customer data that has been stripped of data on a specific customer. Such aggregated data may be provided to third parties.

⁷ The goal of the Children’s Online Privacy Protection Act (COPPA) is to place parents in control over what information is collected from their children online. With few exceptions, the related Federal Trade Commission (FTC) rule requires operators of commercial websites and online services to provide notice and obtain verifiable parental consent prior to collecting personal information from children under the age of thirteen. Parents must also have the right to review or delete a child’s personal information. Since some users of Metro Connect’s commercial online services will known to be under the age of thirteen, Metro Connect is required to fully comply with COPPA. For more information, please see the FTC’s COPPA Web site at <http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>.

⁸ Communications Assistance for Law Enforcement Act (CALEA) – This law, which was passed in 1994, requires that digitally switched telephone networks must be built to enable wiretapping by the Government. The U.S. Department of Justice is in charge of determining the appropriate technology standards. The law provided a specific exemption for “information services”. However, in response to a request from the Federal Bureau of Investigation (FBI) in August 2005, the FCC ruled that broadband voice over IP (VoIP) must also comply with CALEA.

⁹ The Electronic Communications Privacy Act (ECPA) – This law governs the ability of the U.S. government to obtain personal information from an internet service provider.

¹⁰ USA PATRIOT ACT – This law, enacted in 2001 after the World Trade Center attacks, significantly expands the ability of the U.S. government to conduct electronic surveillance operations and to combat the use of telecommunications infrastructure to transmit money to groups with interests adverse to the United States.

b. California

- i. California Constitution, Article 1, section 1¹¹
- ii. Civil Code Sections 1798.80 – 1798.84
 - 1) Section 1798.80
 - 2) Section 1798.81 – Destruction of Records
 - 3) Section 1798.81.5 – Reasonable Security Procedures; Contract Required for Similar Protection upon Disclosure¹²
 - 4) Section 1798.82 – Disclosure of Breach Insecurity by Business Maintaining Computerized Data that Includes Personal Information
 - 5) Section 1798.83 – Disclosure to Customer on Request of Personal Information Provided to Third Parties for Direct Marketing Purposes
- iii. Public Utilities Code Sections 2891-2894.10 (“Telecommunications Consumer Privacy”)¹³
- iv. Business and Professions Code Sections 22575 – 22579 (“Online Privacy Protection Act of 2003”)¹⁴

Metro Connect agrees to comply with all laws, whether or not listed above. Because the area of wireless and broadband technology is in a state of rapid evolution and change, it is foreseeable that the applicable statutes and laws may be amended or changed in the foreseeable future. As such, Metro Connect acknowledges that it is solely responsible for **monitoring continuing developments** in both federal and California laws and remaining in compliance with any new

¹¹ CAL CONST. Article 1, section 1: The state Constitution gives each citizen an "inalienable right" to pursue and obtain "privacy."

¹² Security of Personal Information – CAL CIV. CODE §1798.81.5. This law requires specified businesses to use safeguards to ensure the security of Californians’ personal information (defined as name plus SSN, driver’s license/state ID, financial account number) and to contractually require third parties to do the same. It does not apply to businesses that are subject to certain other information security laws.

¹³ Telecommunications Customer Privacy – Public Utilities Code Sections 2891 – 2894.10. This law bars telecommunications companies from disclosing the calling patterns, personal financial information or other specified personal information of residential subscribers without first getting written consent of the subscriber. There are some exceptions, including disclosure for the purpose of debt collection, for responding to a 911 call, and as required by legal process. It also requires, among other things, that telephone companies must give annual notice to subscribers that calling an 800 or 900 number may result in the disclosure of the subscriber’s telephone number to the called party.

¹⁴ Online Privacy Protection Act of 2003 – Business and Professions Code Sections 22575 – 22579. This law requires operators of commercial web sites or online services that collect personal information on California residents through a web site to conspicuously post a privacy policy on the site and to comply with its policy. The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information. An operator is in violation for failure to post a policy within 30 days of being notified of noncompliance, or if the operator either knowingly and willfully or negligently and materially fails to comply with the provisions of its policy. This law took effect July 1, 2004.

laws or changes in existing laws.¹⁵ Failure to comply with applicable laws shall be deemed a breach of this agreement.

E. Retention of User Information¹⁶

1. Advertising related data

Data obtained for the purposes of advertising to users must be retained in a form incapable of merger with registration, usage, service and location information and may be retained for up to 30 days. However, data obtained for advertising purposes is not required to be retained.¹⁷

2. User specific service related data

User specific service related data obtained for the purpose of network monitoring, security, or operations may only be retained if network abuse is suspected or if required to comply with duly authorized local, state, or federal subpoenas, warrants or court orders¹⁸ and

¹⁵ Wireless Silicon Valley should not have the obligation to adequately monitor ongoing changes and developments in the law. Because Metro Connect will be benefiting by offering wireless technology to users, Metro Connect should bear the responsibility of monitoring changes in law.

¹⁶ Since advertising will support the operation of the network, there must be the potential to monetize traffic. The ACLU advocated a data retention policy of one day for advertising related data. This is because they thought that the data could not be separated from network and user-specific data. While there need to be limits, the lack of ability to consolidate data allows us to relax the requirement to a 30 day disposal policy (First In, First Out). This should allow a significant advertising profile to be created that is useful for revenue generation, while assuring users that data related to their surfing habits will not be retained for a period long enough to identify them.

Note: If cookie technology is used, the user will be able to delete the cookie to stop tracking for that particular anonymous user profile, forcing the ad server to generate a new cookie for the user. This assumes that the provider assigns IP addresses based on DHCP (Dynamic Host Control/Configuration Protocol) or that the ad server is not tracking based on IP address, as we have suggested as a requirement. Deleting the cookie does not, however delete the information stored on the server that was collected based upon that cookie. It does disassociate the user with that anonymous profile however.

¹⁷ Registration data and data related to the use of the service such as login location, IP address and user ID can be maintained in a standard database that is not accessible to any server delivering advertisements. The ad server (even if not run by a third party) can be set up to utilize cookie or similar technology to track only websites visited by users. As long as the data collected by the advertising server(s) are lacking specific user-identifying information such as IP address (or client ID traceable to IP address) or login ID the data will not be a threat to privacy. The key is to avoid collecting such data in the first place. If the data is collected, the temptation to consolidate the data will be too great.

¹⁸ While most of the discussion of monetizing data thus far has been centered on the possible violation of privacy by the advertising itself or advertising entity if separate from the service provider, we now turn to violations that are more direct. Users need to be confident that their personal information provided when they sign up, as well as network usage data (such as log-on frequency and duration) are not sold, traded or provided to third parties for any reason other than acceptable law enforcement activity as discussed in this document. One of the main reasons for this requirement is that the local municipalities are sponsoring the building of this network and contracting with the service provider for the delivery of services. The process should not result in the bargaining away of privacy rights to the government. This was a primary concern of the ACLU.

may only be retained for 30 days unless legal action is taken against the user for which the data is required.¹⁹

III. CONSTRAINTS ON ACCESS TO AND USE OF INFORMATION BY THIRD PARTIES

A. Legal Process, Civil and Criminal

User registration, service, usage, and location information will not be disclosed unless required to comply with duly authorized local, state, or federal subpoenas, warrants or court orders or when necessary to investigate, protect against or prosecute fraud or abuse on the network. Only the information requested in compliance with the Electronic Communications Privacy Act shall be supplied.²⁰ Notice of the information requested in the subpoena, warrant, or

¹⁹ Since it is common practice to monitor networks for reasons related to performance and outage management, such monitoring must be allowed. Most of the data required for these purposes can be consolidated into data groups related to the network itself however, so user specific information is rarely required to be maintained for long durations. For this reason, network traffic data that contains no user specific data may be maintained in consolidated form in such a way that identifies traffic patterns of particular access points, routers and switches should be kept as long as the provider sees fit. User specific data should only be kept when a user is suspected of abusing the network. Under these circumstances data should be maintained for up to 30 days and may be used only for network management purposes, such as determining whether or not a user is abusing the system. Only if the data is required for pending litigation against the user, data retention time will be extended as needed.

²⁰ The Electronic Communications Privacy Act (ECPA) requires that a government entity seeking user information from an internet service provider must do so by warrant, court order, subpoena, or consent of the subscriber. The ECPA contains two main classifications of user information. The first main classification is non-content based information which includes basic user information such as name and address and transactional information such as web addresses visited by the user and email addresses corresponding with the user. The second main classification is content based information which includes the actual information sent or received by the user. The type of legal process required depends upon whether the information requested is content or non-content based.

Basic Non-Content Based Information:

Basic non-content information is available to the government in response to an administrative, grand jury, or trial subpoena. Under these forms of subpoenas, a government entity may request: 1. name; 2. address; 3. session times; 4. length of service and type of service; 5. any temporarily assigned network address; 6. means and source of payment for the service including bank account or credit card number. *See* 18 U.S.C. § 2703(c)(2). As to a temporarily assigned network address, the address is generally considered to be for a particular session as opposed to all of the addresses assigned to the user. Orin Kerr, Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, § III.C.1 at 90 (2002), at <http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf>.

Transactional Non-Content Based Information:

For transactional records, the government must use a warrant or a court order as specified in 18 U.S.C. § 2703(d) which requires the government to show "specific and articulable facts" showing that there are reasonable grounds to believe that the information requested are relevant and material to an ongoing criminal investigation. *See* 18 U.S.C. § 2703(d). The ECPA also allows the government to use "pen register" (identifying outgoing communications) and "trap and trace" (identifying incoming communications) orders to obtain IP addresses, port numbers, and the "to" and "from" fields in an email. *See* 18 U.S.C. § 3127(3). However, content based information such as the body of the email or the subject line are not included as part of a "pen register" or "trap and trace" order.

A provider, however, is allowed to use pen register or trap and trace software and hardware on its own initiative in the following circumstances: 1. for the operation, maintenance, or testing of their service; 2. to protect the provider's property; 3. to protect users from unlawful or fraudulent use of the service; 4. or with the user's consent. *See* 18 U.S.C. § 3121(b).

court order shall be given to the user as soon as possible but in any event, within two weeks of the request via email unless Metro Connect is specifically forbidden from providing user notification by statute or court order.²¹ In addition, Metro Connect shall allow the user a period of three weeks from the date of notice to challenge the request before Metro Connect complies.

B. Protection of User Account Information

Metro Connect shall maintain reasonable security procedures and practices to protect registration, service, usage and location information (user account information) from unauthorized use in compliance with California Civil Code Section 1798.81.5(b).²² The duty to maintain reasonable security procedures and practices to protect user account information shall extend to Metro Connect's contracting parties in compliance with California Civil Code Section 1798.81.5(c).²³ In the event of a security breach compromising user account information, Metro

The ECPA also allows for an internet service provider to disclose non-content based information to the government at the provider's discretion given one of three circumstances: 1. with the user's consent; 2. where the disclosure is necessary to protect the provider's rights or property; and 3. if the provider believes it is necessary to disclose the non-content user information to prevent death or serious bodily injury to another. *See* 18 U.S.C. § 2702(c). The disclosure of non-content based information to private parties is also largely left up to the discretion of the provider by the limits of its privacy policy.

Although Metro Connect may decide in its own discretion whether to provide non-content based information to the government or to private parties without a warrant, the model privacy policy requires a subpoena for legal requests for user information to prevent liability for unauthorized use of user information. Content based communication, however, is specifically not to be disclosed to private parties under 18 U.S.C. § 2702(a).

Content Based Information:

Whether or not Metro Connect decides to provide users with storage space for websites or email accounts will determine whether or not Metro Connect would be capable and therefore responsible for providing content based information to government entities. If Metro Connect were to provide users with storage space for emails, the content of emails stored for less than 180 days could be obtained by the government only with a search warrant. *See* 18 U.S.C. § 2510(17). For stored communications over 180 days, the legal process is less stringent and the government may obtain the content of those emails with a subpoena but the government would be required to provide notice to the user within 90 days.

²¹ Although the law does not currently require providers to notify users when non-content based information has been requested by a civil litigant or private party, the model privacy policy adopts the current industry standard of notifying users of legal requests for information. This industry standard may also be adopted as law in the near future given past California legislative debate. *See* A.B. 1143, 2003 Leg., 2003-04 Reg. Sess. (Cal. 2003).

²² California Civil Code Section 1789.81.5(b) requires businesses that own or license personal information about California residents to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." However, personal information only includes the use of a name when combined with a social security number, driver's license number, California ID card number, medical information, or a means of accessing a user's financial account. *See* Cal. Civ. Code § 1789.81.5(c). Therefore, compliance with section 1789.81.5(b) would only be required if users were identified by credit card, bank account, social security or driver's license/California ID card in addition to their names. However, the use of reasonable security measures is recommended even if personal information as defined in section 1798.81.5 is not collected in order to remain compliant with any future legislation and to reduce Metro Connect's liability.

²³ The requirement to implement and maintain reasonable security procedures and practices also extends to Metro Connect's contracting parties who maintain user information. Section 1789.81.5(c) obligates providers to require by contract that any parties maintaining user information use reasonable security procedures and practices to protect users' personal information.

Connect shall notify the affected users to the extent possible in accordance with California Civil Code Section 1798.82(a).²⁴

IV. REPORTING REQUIREMENTS

Metro Connect shall provide an annual report to Wireless Silicon Valley detailing the number of users for which Metro Connect on its own initiative instituted additional monitoring and or data logging. In addition, the annual report shall detail the number and types of instances of network fraud or abuse Metro Connect reported to law enforcement authorities and the ultimate disposition of such complaints by law enforcement authorities.

V. USER RESPONSIBILITIES

The User must promptly notify Metro Connect of any breach of security related to service, including but not limited to the unauthorized use of the User's account.

Metro Connect shall not be responsible for the safekeeping of any information the user discloses in public areas of any Metro Connect web site or the Internet, including but not limited to: message boards, online forums or social networking sites. Metro Connect shall encourage the user to exercise caution when deciding to disclose personal information in such areas.

²⁴ Under California Civil Code Section 1789.82(a) any business that owns or licenses computerized data that includes personal information, must “disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” Cal. Civ. Code § 1789.82(a). The code also provides that “[t]he disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” Cal. Civ. Code § 1789.82(a). According to Section 1789.82(g), notice can be either written or electronic notice that conforms to the provisions for electronic records and signatures in 15 U.S.C. Section 7001. Similar to maintaining reasonable security measures, if Metro Connect were to license users' personal information or allow any other company to maintain computerized data that includes users' personal information, that company must also notify Metro Connect immediately if there is any breach of security where personal information is reasonably believed to have been acquired by an unauthorized party. *See* Cal. Civ. Code § 1789.82(b).