

Proposed Contract Terms and Privacy Policy for Silicon Valley Metro Connect

Prepared by

**Travis Brandon
Thomas Nosewicz
Jon Novotny
Elspeth J. Simpson
Sarah Tierney**

**Student Fellows
Center for Internet and Society
Stanford Law School**

**Contact:
Lauren Gelman
650-724-3358
gelman@stanford.edu
Associate Director
Center for Internet and Society
Stanford Law School**

PROPOSED CONTRACT TERMS

Service Agreement:

This is a Service Agreement between MetroConnect and Municipal Governments (...) dated *.

1. Definitions

“Customer” means all users of the wireless network, regardless of their level of service.

“Privacy Policy” means the rules that MetroConnect will follow with regards to Customer privacy, as set forth in Appendix A.

2. Service

MetroConnect shall provide service to Customers subject to the Privacy Policy. Any changes to the Privacy Policy are subject to the conditions specified therein.

3. Third Party Beneficiaries

The provisions of the Agreement are for the benefit of the Customers.

4. Breach and Remedies

Each of the following constitutes a breach of the Agreement:

- a) MetroConnect fails in its duty of care to protect Customer information as described in the Privacy Policy with the result that Customer information is exposed or released to a third party.
- b) MetroConnect discloses Customer information to law enforcement or other third parties, except as required by law or under the conditions specified in the Privacy Policy.

MetroConnect's liability for damages to the Customer for any reason due to a breach of Agreement or other cause of action related to the Service shall not be limited except as provided by law.

5. Assignment

This Agreement shall be binding on the Parties and their respective successors and assigns.

PROPOSED PRIVACY POLICY

Exhibit A, Silicon Valley MetroConnect Privacy Policy:

This Privacy Policy was last revised on * and is effective as of *.

MetroConnect Privacy Pledge:

We recognize that privacy is a right guaranteed to California citizens by the California constitution. We've created this Privacy Policy to demonstrate our firm commitment to your privacy and the security of your data.

This Privacy Policy describes how MetroConnect collects information from users of Silicon Valley MetroConnect ("SVMC" or "MetroConnect") wireless network, how we use the information we collect, and the choices you have concerning the collection and use of such information. Please read this Privacy Policy carefully.

Please contact xxx@xxx.com if you have any questions.

1. Definitions

"*User*" means any person or entity using the Service.

"*The Service*" means the lawful connection to the Internet through the SVMC wireless network. Users may access the service in two ways:

Free Service. Users may use the Service "free," that is, without paying a monetary fee to SVMC. When using the Service free, Users will not be required to supply any personally identifiable information to SVMC. The free Service will not allow the full range of activities on the Internet, and will offer limited bandwidth. Users who use the free Service will see advertisements specially inserted by SVMC to offset the costs of the connection.

Paid Service. Users may also use the Service by paying a fee. Paid Users will experience faster and more complete Internet access. Paid Users must provide certain information when they sign up, such as name, address, telephone number, and billing information. Paid Users will have the option to use the free Service, during which time their activities online will not be associated with their paid user accounts.

"*Personally Identifiable Information*" means information about a User that can be used, alone or in combination, to identify that User personally. Such information includes, but is not limited to, the User's name, address, telephone number, e-mail address, credit card number, user name, and password.

"*Customer Usage Data*" means data collected about a User's activities while using the Service, including the individual websites a User visits and the time and duration of Service use. Users may opt-out [add hyperlink] of the gathering, use, or disclosure of this data for certain commercial purposes.

“*Location Data*” means Customer Usage Data, such as IP address or node location, that can be used to determine a User’s approximate location.

“*Aggregate Data*” means data that results from aggregation, a process whereby usage statistics are compiled by stripping personally identifiable user information from usage logs and combining the data in a common pool before analysis. Aggregate Data is maintained in a way such that individual Users cannot be identified.

“*Affiliate*” means any parent company, subsidiary, joint venture, or other company controlled by, or under a common control with, MetroConnect.

“*Third Party*” refers to any entity not affiliated with MetroConnect. Specific varieties of Third Parties include:

Technical Partners. This category refers to a Third Party that contracts with MetroConnect to ensure operation of the SVMC network. Technical Partners are held to the standards of this Privacy Policy by contract.

Promotional Partner. This category refers to a Third Party that enters into a special promotional relationship with SVMC to offer services to Users.

Advertisers. This category refers to a Third Party that pays to display information relating to its own or its clients’ products or services on the SVMC network or websites.

2. Collection and Use of Information:

This section describes what information MetroConnect collects from and about Users, and how MetroConnect uses that information.

Billing Information: Users who sign up for paid Service may be asked to provide certain information at the time of sign up. Such information includes name, address, telephone number, and billing information (i.e., a credit card number). The information collected from Users during the registration process is used to manage each Users’ account (such as billing and collections), and will not be used by MetroConnect for any other commercial purpose.

Customer Usage Data: MetroConnect collects information regarding your use of the Service, including potentially the your physical location and the websites you visit. MetroConnect may use Customer Usage Data (1) to improve the speed, reliability, security and other aspects of the Service and (2) to develop new product offerings. Customer Usage Data will not be combined or stored with Personally Identifiable Data unless a User consents to such storage or combination, or as specifically compelled by law. Users have the option to opt out of some collection and use of Customer Usage Data. Please visit our opt out page [\[hyperlink\]](#) for more information and to exercise this choice.

IP Address: Internet Protocol (“IP”) addresses offer a unique identifier that MetroConnect may use to log User activity across one or more Service sessions. MetroConnect may store non-aggregated IP address data during the data retention period set by this Privacy Policy. Following the data retention period, MetroConnect will convert all Customer Usage Data, including IP addresses, into Aggregate Data, unless otherwise compelled by law.

Location Data: To make wireless communication possible, the network knows the general location of your place of connection. The network must also track your movement and trajectory in order to provide seamless wireless coverage. MetroConnect will use location data to provide wireless service in each session. MetroConnect may also keep location data as Aggregate Data for use in developing products and improving service for Users. MetroConnect, its Affiliates, and Advertisers may use your point of access to target product offers or services to you on an anonymous basis.

MetroConnect may store non-aggregated location data during the data retention period set by this Privacy Policy for the sole purpose of providing it to authorized law enforcement officials under the terms set forth in this Privacy Policy. MetroConnect will not store any non-aggregated user-specific location data for any other purpose except as necessary to provide service in an individual service session or as specifically compelled by law.

Cookie Data. A “cookie” is a small data file that can be placed on your hard drive when you visit certain Web sites. MetroConnect may use cookies to collect, store, and sometimes track information for statistical purposes to operate and improve the products and services we provide and to manage our network and property. MetroConnect will only use “session cookies,” which are cookies that expire at the end of a single session of using the internet.

3. Disclosure of Information:

A. Disclosure of Personally Identifiable Information

MetroConnect may grant access to your Personally Identifiable Information to our employees and agents in the course of operating, developing, and improving our services. We require our employees and agents to use this data only as needed to perform their specific task, and to do so in accordance with this Privacy Policy. These individuals are subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.

MetroConnect will only disclose Personally Identifiable Information about you to Third Parties not under our direct control under the following limited circumstances:

We have your consent. From time to time, you may be given the opportunity to share your Personally Identifiable Information with our affiliates and other third parties through contest entries, surveys, and other means. We require you to opt-in before we will share your information, and will clearly and specifically describe what information is being collected and how we will use it before asking

for your consent.

The Third Party is a Technical Partner. We may disclose your Personally Identifiable Information to technical partners in order to process the information on our behalf. We contractually require that these parties to process your information based on our instructions and in compliance with this Policy and to employ other appropriate confidentiality and security measures.

We in good faith believe the release of information is necessary to comply with applicable law. We will only respond to requests for Personally Identifiable Information from the government, third parties, and the court system that are properly formatted requests in the form of subpoenas, court orders, or warrants and meet all legal requirements necessary for the disclosure of the type of information requested. If we are given such a request, unless prevented by law, we will provide you with notice of the request on the login screen and by e-mail and will give you three weeks to challenge the request before we comply.

We may also disclose user information to enforce or investigate breaches of the SVMC Terms of Service or to protect the MetroConnect network against fraud or other abuse of the network.

Note: Any information that you disclose in public areas of our Web sites or the Internet, including message boards, online forums or social networking sites, may become public information. You should exercise caution when deciding to disclose personal information in these areas.

B) Disclosure of Aggregated Data:

MetroConnect may share Aggregate Data about users with Affiliates and select Third Parties as follows:

Affiliates: MetroConnect will share aggregated information about you with select affiliates to target ads to Users based on their preferences. Affiliates will not be allowed to sell, rent, or gift user information to other parties, or to use MetroConnect data for any purpose not connected with network services.

Technical Partners: To ensure an operational and reliable network, MetroConnect works closely with a range of technical partners. As part of their normal operation, these partners may require detailed information of network usage and other statistics. These partners will be allowed access to this information only in the aggregate and User-identifying information will never be made available to them absent affirmative User consent.

Promotional Partners: MetroConnect may occasionally partner with Affiliates that offer special deals or other offers to MetroConnect Users. These partners will be allowed access to this information only in the aggregate and User-identifying information will never be made available to them absent affirmative User consent.

Advertisers: MetroConnect is funded in part by advertising that is sold and displayed to Users of the service. MetroConnect is able to charge more for advertising if advertisers know which demographics are likely to see their ads. MetroConnect will share aggregated and non-identifying information about its Users collected through the registration process as well as through online surveys and promotions with select advertisers to deliver advertisements tailored to your interests. MetroConnect does not share personal information about its Users with these advertisers absent affirmative user consent.

We also use third-party advertising companies to serve ads when you visit our Web sites. These companies may use information (not including your name, address, email address or telephone number) about your visits to this and other Web sites in order to provide advertisements on this site and other sites about goods and services that may be of interest to you. For more information about this practice and your choices about the use of your data by third-party advertisers, please visit [website].

Unaffiliated Websites: MetroConnect has no control over the data collection and privacy practices of unaffiliated websites to which Users may travel through the Service. Be aware that if you visit non-MetroConnect Web sites where you are prompted to log in or that are customizable, you may be required to accept cookies. We do not control use of these cookies and expressly disclaim responsibility for information collected through them. Please note that cookies can be easily disabled and deleted via your browser's privacy preferences.

4. Data Retention

Personally Identifiable Information and Customer Usage Data will be deleted or converted irrevocably to Aggregate Data after thirty (30) days, except as necessary to maintain network or billing functions. Any non-aggregated data retained beyond the thirty-day limit will be stored in a format that cannot be combined or correlated with Aggregate Data.

5. Amendments to Privacy Policy:

Privacy Task Force: Silicon Valley Wireless will convene a Privacy Taskforce to monitor, suggest, and approve changes to the Privacy Policy. The Privacy Taskforce will consist of representatives from MetroConnect, the municipal governments, NGOs, and academia. All Privacy Taskforce meetings will be open to the public. Any suggested amendments to the Privacy Policy will be open for comment from the public for 90 days prior to a vote. Amendments will be subject to a two-thirds majority vote of the Taskforce.

Notice of Changes to Policy: We will post any changes to the Privacy Policy on this page and will post notice that the Privacy Policy has been changed on our [portal page], where user's must click that they accept the Privacy Policy before logging into the network. Each version of this Policy will be identified at the top of the page by its effective date,

and we will keep prior versions of this Privacy Policy in an archive for your review.

Acquisition: If another company acquires MetroConnect, or acquires assets that comprise or include your personally identifiable user information, that company will assume the rights and obligations regarding your personally identifiable information as described in this Privacy Policy.

6. **MetroConnect's Commitment to Children's Privacy:**

Protecting children's privacy is especially important to us. It is our policy to comply with the Children's Online Privacy Protection Act of 1998 and other applicable laws.

The Service is not directed particularly at children. In recognition of the important privacy interest that children under 18 have, we will not ask for or attempt to collect Personally Identifiable Information from any person whom we have reason to believe is under the age of 18. As we cannot guarantee the privacy and security of children on the Web, however, we recommend parental involvement in any child's use of the Service, particularly concerning the disclosure of personally identifiable information online. For information on children and online privacy assembled by the Federal Trade Commission, please visit this website: <http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>.

7. **Security Pledge:**

We will follow industry best practices for security and internal procedures to secure your data from attack by hackers, pretexters, and other third parties.

8. **How to Access or Modify Your Information:**

MetroConnect offers Users the opportunity to access or modify information provided during registration. To access or modify such information, visit [website].

ANNOTATION

Proposed Contract Terms:

1. **Definitions**

This definition of customer covers all users of the network, including both the free and paid services. The privacy policy should apply to users of the free service because this network is being deployed as a public good, so members of the public who cannot afford a private, paid service should not be required to accept lower privacy standards simply because they cannot pay for them. The privacy policy also should apply to users of the paid service because the costs of service should be reflected in the price, without any "hidden charges" in the form of weaker privacy protections.

2. Service

The terms in the privacy policy should not be amendable except as provided for in the privacy policy itself. Because the terms of the privacy policy will be determined with input from all interested parties, any amendments to the privacy policy should also be determined with similar input (as specified in the policy).

3. Third Party Beneficiaries

Service providers that contract with the government do not have a duty of care to third party beneficiaries. This provision expresses the intent of the parties to create a duty of care to the customer.

4. Breach and Remedies

Provision (a) creates a cause of action for the customer against MetroConnect in the event of a breach of the duty of care. This is the preferred situation because the Municipal Governments will not bear the cost of any litigation regarding breach of the duty of care. Rather, the onus will be on customers to enforce their rights.

Provision (b) creates a cause of action for the customer if MetroConnect breaches the contract (including by violating the privacy policy).

There is no limit on liability because we want to create the proper incentives for MetroConnect to uphold its obligation to protect privacy in accordance with the privacy policy. Placing a limit on liability may induce MetroConnect to breach the policy when the money earned from selling customer information exceeds their maximum liability. This provision also creates an incentive for MetroConnect to use reasonable care in protecting customer information.

5. Assignment

The privacy policy will be binding on any future successors and assigns of MetroConnect, who must negotiate amendments to the privacy policy according to the terms of the policy. This will protect the privacy rights of customers.

ANNOTATED PRIVACY POLICY

MetroConnect Privacy Pledge:

This privacy pledge seeks to balance the concerns of the network with the concerns of individual users of the network who want to prevent the disclosure of their information to third parties. The network will need to share some information to show advertisers that their ads are effective and to allow the cities to monitor overall network usage. However, individuals have a strong interest in preventing disclosure of personally identifiable information to third parties. First, any disclosure of personally identifiable information

infringes on the user's right to privacy--someone they did not authorize now has access to their information. Second, providing information to third parties makes it more likely the user will be subject to additional spam and other mass mailings targeted at them. Third, it is in the user's best interest to limit the number of people who have access to their personally identifiable information. The more people that have access to it, the more likely a leak of that information is possible. In an age where identity theft is becoming common, individuals have a strong desire to take whatever steps are possible to avoid this disclosure.

Collection and Use of Information:

A. Types of Information Collected:

Billing Information: This information is obviously necessary for the network to function for the paid users. Information collected here should be limited: there is no need to collect a social security number, or information about occupation or income.

IP Address: This is the main technique for generating information that is valuable for advertisers. However, care must be exercised in collecting and storing this data. An IP address should never be linked to an individual User's billing information.

Presence, Location, and Tracking: The use of presence, location, and tracking data to target advertising to consumers is yet another major concession to the business needs of the network. As such, it should be justified with an explanation of the costs of running the network and why such advertising is necessary, especially for users who are paying for access to the network already. Location information provides very specific information about where a User is physically located, and this could be used to help identify an individual User. But this information is also very valuable to advertisers: for example, if visitors who are attending a large convention access the wifi network from the convention center or neighboring hotels, this information will allow ads specific to the convention to be targeted at them. This information will also allow ads that a consumer may find particularly useful to be targeted at them: for example, this information could be used to send an ad about a local restaurant to someone who is around the block.

Cookies: Cookies are the main tool that MetroConnect will use to monitor network activity and generate aggregated data that will be useful to advertisers and for maintaining and upgrading the network. It is very important that only "session cookies" are used and that they are purged at the end of each browsing session. A cookie should not become a unique identifier for any particular User.

B. Disclosure of Customer Data:

Although it would be best for information to only be released in the aggregate, we recognize that for time to time it will be necessary for the network to release personally identifiable user information. This section sets forth the rules and boundaries for such disclosures by identifying five categories where disclosure can occur.

Consent: The user can consent to the release of the information. This is potentially a huge privacy concern as networks might try to obtain general, blanket consent at the beginning of service and thus try to get around the protections for personal information. However, the privacy policy will require the network to "clearly and specifically" describe what is being opted-in to. This will prevent the network from getting blanket consent to share the information with anyone it wants to for all time. Allowing release by consent does give the network more flexibility in when it can release information, and thus this represents another compromise between individual interests and the network's interests.

Network Management: The network may release the personally identifiable information to others for help in processing the information. This clause recognizes that the network cannot do everything on its own and may have to turn to others for help. However, by binding those others to the same privacy policy, the individual user's privacy interest is still fairly well protected. The requirement that the same privacy policy be used is essential to protecting all user information that is submitted to the network, not just information that is currently under the network's control.

Legal Process: The privacy policy recognizes that sometimes personally identifiable user information must be shared in order to comply with the legal process. However, far too often ISPs, search engines, and other businesses with large amounts of user data release information too quickly. This section seeks to ensure that personally identifiable information will only be released where it is actually required by law. This is done in two ways.

First, by requiring a properly formatted subpoena, court order, or warrant complying with all applicable law, we ensure that only legitimate requests that have been properly approved are complied with. The last clause of this section does allow user information to be disclosed to enforce or investigate breaches of the system and to protect the network without a properly formatted subpoena, court order, or warrant complying with the law. This is a broad concession done in recognition of the fact that the network owner needs to be able to keep the network running smoothly. However, the network owner should not take advantage of this clause to infringe user privacy more than absolutely necessary to protect the network.

Second, by requiring the network to give the user notice where allowed by law (as opposed to required by law), we give the user the broadest opportunity to object to the disclosure of his or her identity and to argue anonymously before the courts that the subpoena should be squashed. This is an important part of our legal system that cannot be used if the information is released automatically. The importance of notice provisions has already been recognized by at least two states--Virginia and Arkansas--which require service providers to give users notice before turning over personally identifiable information. Notice provided at the time of login should be prominent and designed to catch the user's attention.

There are several ways the government and third parties can request information. The following summarizes the categories laid out in the EFF's Online Service Provider Best Practices document available at http://www.eff.org/osp/20040819_OSPBestPractices.pdf:

Law Enforcement: Law enforcement officials are required to obtain subpoenas, warrants, or court orders before obtaining personally identifiable information from ISPs. Although only a subpoena is required to obtain basic subscriber information, a warrant or court order is required for more detailed information such as the user's identity, what URLs he visited, what he searched for, or e-mail content.

Subscriber Information: Civil and criminal subpoenas can also be issued for "subscriber information" including name, address, phone number, etc. Usually, these are issued to discover the identity of someone posting anonymous comments (for instance, an employer trying to determine who is saying bad things about the company). Sometimes these are sought merely for harassment, and sometimes they form the basis of later legal action.

DMCA Subpoena to Identify Infringer: This civil subpoena is issued to service providers allegedly hosting material that infringes copyright under the DMCA. No lawsuit has to have been filed (unlike a normal subpoena) but a notification of alleged infringement with specific requirements is required. This type of subpoena likely will not apply to this case since the wireless network is only providing connectivity, not hosting infringing works.

Requests Without Properly Formatted Subpoena, Court Order, or Warrant: Sometimes individuals may request information about a user, claiming that user has engaged in harassment or other bad acts. Although the service provider may feel sympathy for the individual, the truth of the story cannot be verified and releasing the information without a properly formatted legal request can subject

the service provider to liability from the user. This is why requiring a subpoena, court order, or warrant is so important for the network.

Employees, Contractors, and Agents: The policy next recognizes that in the real world, employees of the company may have a need to access user information. However, by restricting the uses of that information to activities required by the company and providing that action can be taken against those who fail to act in accordance with company policy, the privacy policy tries to strike a balance between business needs and protecting user privacy to the utmost.

Public Areas of Website: This section is included to make it clear that the network is not responsible for information that the user voluntarily shares through bulletin boards, forums, and other similar sites.

C. Disclosure of Aggregated Data:

This section focuses the limited set of entities with which the network will share aggregated data. Because of the strong privacy concerns associated with sharing user data with third-parties, many of whom will not be parties to this privacy policy, it is important to reiterate that only aggregate data, never personally identifying data, should be shared

with third-parties. This policy is followed by companies such as Google, the New York Times, and TiVo, among others.

Affiliates: Despite the close legal and financial relationships the network shares with its affiliates, personal user data should remain segregated within MetroConnect. Personally identifiable user information should only be shared with affiliates after obtaining the user's consent, as in Section B above. Otherwise, only aggregated data should be shared.

Technical Partners: This clause describes how aggregated data will be shared in order to maintain the network. Specific user-related technical problems will be handled under the restrictions described in the section above.

Promotional Partners, Advertisers, Ad Serving Companies: MetroConnect is largely funded by advertising sold and displayed to users. While this is necessary to the operation of the system, it is vital that user privacy be thoroughly protected in the process. To this end, only aggregated information should be shared with any of these groups. Information used for advertisement targeting should not be collected in such a way as to allow profiling of identifiable individuals. Users should be given clear notice of how to opt out of these practices.

Unaffiliated Websites: This section makes clear that MetroConnect is not responsible for aggregated user data collected by unaffiliated websites.

Amendments to Privacy Policy:

The intention of the Privacy Task Force is to create a group that will have members of Municipal Governments, MetroConnect, citizen groups and academia that can thoughtfully consider any amendments to the privacy policy. The Task Force will also serve as a body to which citizens can comment. The required two-thirds majority will ensure that amendments to the privacy policy have been thoroughly discussed and agreed upon by a super-majority.

Any changes to the policy should be accessible on the web along with the previous versions of the Privacy Policy for purposes of comparison. Customers will have to accept these changes to ensure that they have read the new policy. This is necessary to inform Customers of their rights.

Any entity that acquires assets governed by the Privacy Policy will assume rights and obligations under the policy. This ensures that neither MetroConnect nor its successors or assigns cannot outsource mining of private data. It also will protect the rights of Customers in the event of an acquisition. Holding user privacy to the same standards of care across time is extremely important because users rely on the privacy policy while using the network, despite any change of network ownership.

Security Pledge:

There is a risk of hackers and other security breaches wherever data is stored. It would be

difficult to hold the network liable for every single breach that happens, as many cannot be anticipated. However, by requiring the network to follow best practices for security and internal procedures, we make the success of hackers less likely. These best practices should include physical data security as well as policies and procedures governing when information is disclosed to avoid phenomena such as pretexting, where a third party pretends to be a network user in order to get additional information from the network.

We recognize that there is no way for the network to guarantee there will never be a security breach. However, it is important that third parties have a cause of action in situations where the network fails to take proper precautions and there is a security breach. There must be a guarantee of some security support for users' privacy.

While we do not think the privacy debate should focus on matters of security, it is worth noting a few things about the proposed system:

Information can be encrypted both going to the wireless access points and across the network. The proposal made by SeaKay, IBM, Cisco, and AzulStar states that the Cisco Access points will support WPA2 encryption as well as WPA encryption from customer laptops (so the transmission of data from the user's laptop to the access point is secure). In addition, the network will use AES encryption to ensure data is secure across the network.

The quality/type of encryption may vary by levels. According to SeaKay, IBM, Cisco, and AzulStar's proposal, the type of encryption used may vary by user group and thus those with the least bargaining power (at the free level of access) may have trouble pushing for higher levels of secured access. However, the network as it stands now will guarantee all users at least WPA encryption.

Here is the break down by levels:

- * Free users can chose between Open or WPA
- * Kids can choose between Open or WPA
- * Entry users can choose between Open/WPA
- * Extreme users can choose between Open/WPA/and WPA2 RADIUS
- * Pro users can choose between WPA2 and Radius
- * VoIP users have WPA2.

This is not the only way to secure the transmission of user data. At least one other municipal wifi network (Google's network in Mountain View) has an open, unencrypted wifi network but offers a free virtual private networking (VPN) client to allow people to have security on the network.

The proposal by SeaKay, IBM, Cisco, and AzulStar states that VPN tunnels will be available to further secure communication for city government and public safety, but does not mention any additional uses--like customer use. Therefore, it is unlikely that the SeaKay, IBM, Cisco, and AzulStar system will provide VPN to its regular users.

Leaving aside any technical differences or limitations on the two methods of protecting

user data, it is important to note that the promise that the network itself will be encrypted may place more of a burden on the network provider than the provision of a VPN client which users are free to choose whether or not they will use. Therefore, we would expect the network providers to face liability for failure to secure the network as promised.