DATA FOUNDRY

Senate Business and Commerce Committee
Interim Hearing
August 14, 2012
Andrew Macfarlane
Data Foundry, Inc

Good Afternoon Mr. Chairman, Members and esteemed guests and visitors. My name is Andy Macfarlane and I work for and represent Data Foundry, Inc. Data Foundry is a facilities-based data center operator headquartered in Austin and we own and operate with 3 data centers in Texas. We also serve customers from data centers in Virginia, Florida, California, The Netherlands, Germany, Great Britain and Hong Kong. We serve customers in approximately 214 countries

Recent studies and surveys predict good things in the long term for the fiber optical networking market, thanks to increasing bandwidth demands from data centers. The new bandwidth driver is data centers. Large-scale data centers continue to be built out – both the multi-tenant, carrier-neutral variety and private data centers. Sales of fiber-optic network systems will grow at a 5% compound annual growth rate through 2017, to reach $20 billion, according to Market research consultancy Ovum.

Data Foundry's customers and their patrons have traditional privileges, contractual nondisclosure agreements and statutory obligations to maintain confidentiality of corporate, governmental and individual consumer proprietary information. They have confidential/trade secret information, which is their property. They use the Internet to transmit confidential information on a regular basis and until recently had no concern whether their underlying transmission provider would somehow destroy this confidentiality by inspecting and appropriating the content or reserving the right to do so.

With Internet access providers (IAPs) increasingly inspecting network traffic, more and more companies will soon be taking their confidential information and communications offline, and returning to traditional, inefficient means of conducting business. Should businesses continue to abandon the Internet for the carriage of their most important and sensitive data, the repercussions for E-commerce would be significant and widespread.

When IAPs implement policies that require customers to consent to wholesale network inspection as a mandatory condition of service, IAPs present businesses with an unfortunate dilemma. They must choose between disclosing their privileged information to their IAP or they can protect the privacy of this material by conducting business entirely offline. Any prudent business will choose the latter even though that means sacrificing the benefits associated with the Internet. The risk of losing the confidentiality of their proprietary information is simply too great and costly. This abandonment of the efficiency and utility of the Internet would mark a significant step backwards for E-commerce and hurt the economy as a whole. Cloud computing, Email, web browsing, downloads, E-transactions, all create information that users expect to remain private.

We believe that for Cloud Computing to remain an integral part of our nation's economy, proprietary business information must remain secure and confidential as it travels the Internet. Privacy promotes autonomy, free expression, and free association on the Net. Privacy also fosters non-mainstream ideas, tinkering, and, ultimately, innovation.

Users expect privacy and the Internet has always been private. Individual users and businesses operate on the Net under the assumption that nobody will be watching and reading their mail. Businesses can communicate about proprietary processes. Lawyers and clients can communicate in confidence, as well as doctors and patients. Users can feel free to purchase things with their credit cards online. Users can browse unsavory content and explore unpopular ideas without fear of anyone finding out. This is how an open Internet should operate in a free society.

I think it's important to note that to note that IAPs are essentially middle-men. They are third parties to all online communications, which is different than Google. When you do a Google search, you understand that Google is the other party to the communication and you obviously don't expect Google not to see the search. With IAPs, you don't expect them to see. They have no right to see, other than the fact that they made you consent to it by making it a mandatory condition of service buried in the contract.

Safeguards are needed to protect private information from network inspection. User privacy should be a default rule on the Net. Users should not be compelled to waive their privacy as a mandatory condition of service. Any waiver of privacy should be opt-in and totally voluntary.

Users should have the ability to hold their network providers accountable for any violations of their privacy rights. They shouldn't be able to bury waivers of privacy in contracts. User rights should prevail over the IAPs pecuniary interests. If the IAPs give the users a good enough reason to forfeit their privacy (e.g. parental controls), then the users are free to sign away their privacy, so long as it is an informed decision. **Users should have to take affirmative steps to lose their privacy**.

DATA FOUNDRY

Here is an example of one provider in Texas and their TOS:

http://www.centurylink.com/Pages/AboutUs/Legal/PrivacyPolicy/

Network management:

We use information generated on our networks to manage those networks, to plan for future development, and to keep our services running reliably and efficiently. For example, we monitor data to check for viruses, to control spam, to prevent attacks that might disable our services, to ensure that your traffic does not violate your subscriber agreement or our acceptable use policies, and to guard against other inappropriate or illegal activity. This may involve looking at the characteristics of our network traffic, such as traffic volumes, beginning and ending points of transmissions, and the types of applications being used to send traffic across our network. In limited circumstances**, we need to look into the content of the data** (such as the specific websites being visited, files being transmitted, or application being used) for the purposes described above, in circumstances when we are concerned about fraud or harassment, to repair a problem we detect or that a customer contacts us about, or when we are providing the content of broadband traffic to law enforcement which we only do as authorized by law.

As your ISP, we gather and use information as outlined above under General Practices.

Information we obtain when CenturyLink provides Internet access:

We gather and use information generated on our networks to manage them, to plan for future development of our network and services, to market our services, and to keep our services running efficiently. For example, we monitor data to check for viruses, to control spam, to prevent attacks that might disable our services, to ensure that your traffic does not violate your subscriber agreement or our acceptable use

policies, and to guard against other inappropriate or illegal activity. This involves looking at the characteristics of our network traffic, such as traffic volumes, beginning and ending points of transmissions, and the types of applications being used to send traffic across our network.

Sometimes we need to look into the content of the data (such as the specific websites being visited, files being transmitted, or application being used) for the purposes described above, in circumstances when we are concerned about fraud or harassment, to repair a problem we detect or that a customer contacts us about, or when we are providing the content of broadband traffic to law enforcement which we only do as authorized by law.

Most of the specific information we obtain that is attributable to a user is kept only for a matter of hours or days. We may retain data for longer if, for example, we see patterns in the traffic that give us concerns about potential harm to our network, or if we are doing a specific study on the impact of certain applications used on our networks. We also retain for longer periods logs of the total amounts of data transmitted, and the date, time, and duration of access to the Internet through our services by a user, including the user's IP address at the time.

We will not look into the content of your email, websites visited or other communications **for marketing purposes** without first informing you and giving you a choice about whether you want us to do so. (This gives them the right to look at content for non-marketing purposes).

We're not picking on CenturyLink in particular. This is just an example of what many providers put in their contracts. My time is up and I'm grateful for the opportunity to visit with you today. I would be happy to supply to the Committee a list of questions to help determine how Texans can best protect our privacy on the Internet.