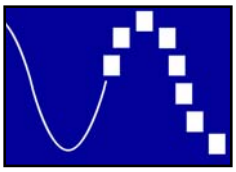
December 17, 2007



The VON Coalition

Honorable Kevin J. Martin
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Implementation of the Telecommunications Act of 1996-Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information, CC Docket No. 96-115

Dear Chairman Martin:

The Voice on the Net Coalition ("VON Coalition") files this ex parte submission regarding the FCC's consideration of proposals to restrict or ban foreign storage of and access to customer proprietary network information (CPNI) generated in the United States.

The VON Coalition supports the Commission's goal of protecting confidential customer data against unauthorized release. Interconnected Voice over Internet Protocol (VoIP) providers are working hard to implement the Commission's recently adopted application of CPNI requirements to them. However, the VON Coalition is concerned that the Commission may adopt new rules, utilizing a stale record developed years before the Commission even defined Interconnected VoIP, and without adequately considering the full implications of applying such restrictions to communications based on a global network. The Commission should not implement any ban on foreign storage of or access to CPNI, and in particular should not apply any such ban to providers of Interconnected VoIP services or any other IP service.

1. The Commission Should Refresh the Record

The record in the proceeding regarding this proposal was originally established in 1998, in response to a proposal made by the FBI in 1997. When the Commission last sought industry comment on this proposal in 2002, no party could or did expect that the Commission would apply CPNI rules to Interconnected VoIP. Even today, Interconnected VoIP providers are still in the process of implementing the Commission's April 2007 order applying CPNI regulations to them. Thus, the record in this proceeding is seriously incomplete.

Moreover, from 1997 to the present, the parties which proposed to restrict foreign storage of CPNI, the Department of Justice (DOJ) and the FBI, have never identified any issues or problems engendered by foreign CPNI storage or access by Interconnected VoIP providers. During this period, the VOIP industry has implemented robust privacy safeguards, including those CPNI safeguards adopted by the Commission this year, to protect against unauthorized access to customer information. VoIP-based services have grown into an industry of global scope with global customers, who use this IT-based business tool to help their competitiveness in global markets.

Before reaching a decision regarding foreign storage and access to CPNI, the Commission should refresh the record. Refreshing the record would enable DOJ and the FBI to state any concerns they may still have regarding storage of or access to CPNI, and would enable Interconnected VOIP providers and their customers to provide concrete information regarding the present and future economic impact of the restrictions proposed by the DOJ and FBI. Refreshing the record would also facilitate a discussion of the impact of these proposed restrictions on U.S. international trade obligations.

2. Section 222 Does Not Provide A Legal Basis for Restricting CPNI Storage or Access For Security Reasons

As the Commission explained in its order of April 2007, Section 222 of the Communications Act, which is entitled "Privacy of customer information," requires telecommunications carriers to protect the confidentiality and privacy of their customers. As its title indicates, Section 222 concerns privacy issues, and does not authorize the Commission to restrict foreign access to, or storage of, domestic CPNI for security or law enforcement reasons.

Section 222 is designed to address consumer privacy, not to ensure that CPNI is optimally available for law enforcement. Only Congress can give DOJ and the FBI what they are requesting. Indeed, we are not aware of any similar requirement that has been imposed on the records or information of service providers in other industries, including, for example, financial institutions.

3. The DOJ and the FBI Have Not Demonstrated the Existence of Any Actual Problems Regarding Foreign Storage of or Access to U.S. CPNI

The DOJ and the FBI have not adequately shown that there is an actual problem regarding U.S. government access to CPNI of U.S. customers stored abroad, or pretexting/privacy issues directly attributable to non-U.S. operations. Furthermore, there is no reason to believe that law enforcement officials are not now gaining access to the call detail records (CDR) they need to conduct investigations – even when those records are held abroad.

Furthermore, the DOJ and the FBI have not demonstrated the existence of problems flowing from foreign storage of CPNI by Interconnected VoIP providers or their customers, or from access to CPNI by IT-based businesses or their customers from points abroad. Interconnected VoIP providers implemented stringent controls regarding accessing of information well before the Commission's April 2007 order. Globally networked IT businesses have globally implemented integrated state-of-the-art security measures. For example, Interconnected VoIP providers have often implemented a variety of robust privacy safeguards to protect against unauthorized access to customer information. Companies are using cutting-edge Internet technologies to provide comprehensive privacy protections for their Internet Protocol ("IP")-enabled products – often utilizing encryption and authentication technologies to protect customer data. When highly confidential information (such as a credit card number or password) is transmitted over the Internet, for example, companies protect such information through the use of encryption, such as the secure socket layer ("SSL") protocol common to Internet e-commerce transactions.[1] In a

[1] VoIP providers also often utilize security measures such as electronic "keys" and/or "locks," digital signatures, and on-line fraud management solutions.

dynamic industry, Internet companies are constantly revising and re-evaluating such procedures to enhance these safeguards and keep a step ahead of the pretexters and protect customer information.

4. The Proposed CPNI Restrictions Would Needlessly Damage the Operations of Global Interconnected VoIP Providers and their Global Customers

The restrictions requested by the DOJ/FBI are completely inconsistent with the international nature of application-based services. Multinational service providers, and their customers in multinational organizations or foreign offices of U.S. organizations, need to be able to access all CPNI generated by such customers, regardless of where it is generated or stored.

Telecommunications carriers may also partner with IT firms to offer non-telecommunications IT services such as presence, desktop integration, or web conferencing to the carriers' customers. These service offerings provide enhanced functionality, wider consumer choice, economies of scale and lower prices to customers. Carriers now lawfully share CPNI with their third-party IT-firm partners to facilitate offering these services, which when they are Internet-based can take place anywhere in the world. Any rule issued by the Commission as a result of this proceeding should not interfere with IT firms' continued third party access to CPNI from their carrier partners.

The U.S. has promoted the free flow of information across borders to enable U.S. businesses to enter and operate effectively in foreign markets. Those businesses would be immediately harmed by restrictions on foreign storage or access to CPNI. A U.S.-based multinational corporation generating jobs in the United States exporting U.S.-origin products and services may contract globally with a provider of Interconnected VoIP services. An interconnected VoIP provider can offer networked global VoIP solutions integrating voice, data and email services. If denied access to CPNI, it may be unable to remotely maintain customers' connections to the service, and prevented from meeting contracted-for standards for network performance.

The real network benefits of allowing foreign CPNI use and storage outweigh the speculative risks raised by law enforcement agencies:

- Geographic diversity
- Disaster recovery
- Business continuity
- Scalability
- Increased efficiency
- Decreased consumer costs
- Increased innovation

For these reasons, we do not believe it to be necessary or prudent to apply any new restrictions on the foreign storage of or access to CPNI generated in the United States of Interconnected VoIP providers.

The proposed ban on foreign storage of or access to U.S. CPNI would also require interconnected VoIP providers to make distinctions that are technically impossible. Because of the nomadic

nature of interconnected VoIP services, an interconnected VoIP customer's actual connection could occur anywhere in the world where there is a broadband connection. If the U.S. restrictions apply to interconnected VoIP providers, they would likely have the effect of forbidding foreign storage of *foreign* CPNI.

No matter what reason the FCC may cite for imposing a ban on foreign storage and access to CPNI, action to apply such a ban to IP-based services such as Interconnected VoIP providers would inevitably prompt other countries to adopt similar measures for their own purposes, whether the U.S. government agrees with those goals or not. The result will Balkanize the Internet, increase consumer costs, deprive global IP communications providers of the productivity benefits of Internet communications, fragment the back offices of their customers, increase frictions between law enforcement agencies regarding control of CPNI, and frustrate U.S. law enforcement agencies' security goals.

As the EU's Data Privacy Directive has shown, other jurisdictions may have conflicting agendas in regulating data storage and use. If FCC requirements were to conflict with privacy or other laws of other jurisdictions, the conflict would place U.S. IT businesses in an untenable position. The FCC should ensure that any order it issues as a result of this proceeding does not conflict with foreign laws or with U.S. international agreements. Refreshing the record in this proceeding would assist the Commission in this task.

While we do not think the Commission should act at this time, if the commission nonetheless does take action we generally agree with the suggestions submitted by Verizon in its August 22, 2007 ex-parte suggesting that 1) any order should be carefully tailored so as to expressly exclude business and multinational customers from any restrictions on foreign storage or access to CPNI, and 2) any order should expressly preserve foreign-based access to CPNI stored in the United States and preserve temporary foreign storage of such CPNI. As Verizon indicates, these exclusions would merely limit – but not entirely eliminate – the vast negative effects of the FBI's proposal on U.S. interconnected VoIP providers' ability to compete internationally and provide effective service, as well as on U.S. trade policy.

5. The Proposed Restrictions Violate U.S. International Trade Obligations and Are Inconsistent with U.S. Trade Policy

The limits proposed by the DOJ and the FBI are inconsistent with both the letter and the spirit of U.S. international trade obligations and policy, under the World Trade Organization (WTO) General Agreement on Trade in Services (GATS) and U.S. free trade agreements (FTAs) with various trading partners.

- U.S. trade commitments under Articles XVI and XVII of the GATS require unconditional market access and non-discriminatory treatment for telecommunications services and IT services supplied cross-border by service suppliers of other WTO Members.
- Paragraph 5(c) of the GATS Annex on Telecommunications requires that such service suppliers must be accorded the right to use telecommunications networks for movement of information across borders and for access to machine-readable information stored in databases in the territory of any WTO Member.
- The U.S. FTAs also provide for market access and non-discriminatory treatment for telecommunications and IT services and service suppliers of FTA partners. And the FTA

provisions on cross-border services forbid a FTA partner from requiring a FTA service supplier to establish or maintain a representative office or any form of enterprise, or to be resident, in its territory as a condition for the cross-border provision of a service.

A ban or restriction on foreign storage of U.S. CPNI, or on access across borders to U.S. CPNI, would be contrary to these trade commitments, and would expose the U.S. Government to being sued by another government or the EU in the WTO or under one of the U.S. FTAs. U.S. exports of goods or services could be subjected to sanctions if the U.S. did not come into compliance with its trade obligations.

Instituting such a ban or restriction would also undercut the success that the United States has achieved in getting U.S. trading partners *not* to impose just such measures. When India proposed to impose guidelines on long distance services that would have restricted transfer outside India of accounting, user and network infrastructure management information, in 2006-07 U.S. negotiators intervened to address these guidelines.[2]

The U.S. Government has consistently urged that concerns like those raised by the FBI and DOJ should be dealt with on a narrowly tailored, case-by-case basis, rather than through any blanket prohibition on cross-border activity. A blanket prohibition on foreign storage or accessing of data, arbitrarily targeted at CPNI and not based on a particularized risk assessment, runs contrary to basic U.S. principles of an open international economy, and could be unsustainable if challenged in the WTO.

Respectfully submitted,

The VON Coalition

cc: Commissioner Michael J. Copps
Commissioner Jonathan S. Adelstein
Commissioner Deborah Taylor Tate
Commissioner Robert McDowell

About the VON Coalition:
The Voice on the Net or VON Coalition consists of leading VoIP companies, on the cutting edge of developing and delivering voice innovations over Internet. The coalition, which includes AT&T, BT Americas, CallSmart, Cisco, Covad, EarthLink, Google, iBasis, i3 Voice and Data, Intel, Intrado, Microsoft, New Global Telecom, PointOne, Pulver.com, Skype, T-Mobile USA, USA Datanet, and Yahoo! works to advance regulatory policies that enable Americans to take advantage of the full promise and potential of VoIP. The Coalition believes that with the right public policies, Internet based voice advances can make talking more affordable, businesses more productive, jobs more plentiful, the Internet more valuable, and Americans more safe and secure. Since its inception, the VON Coalition has promoted pragmatic policy choices for unleashing VoIP's potential. http://www.von.org

[2] http://www.ustr.gov/assets/Trade_Sectors/Telecom-E-commerce/Section_1377/asset_upload_file213_11066.pdf