Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act Of 1966:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information;	)	
	)	
Petition for Rulemaking To Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information	)	RM-11277

To the Commission:

Comments of Nickolaus E. Leggett,
Political Scientist and Electronics Technician

The following are formal comments on the protection of the privacy of customer proprietary network information (CPNI). I have a Master of Arts (MA) degree in Political Science from the Johns Hopkins University. I am a certified electronics technician (ISCET and NARTE) and an Extra Class amateur radio operator (call sign N3NL). I am also an inventor holding three U.S. Patents. My latest patent is a wireless bus for digital devices (U.S. Patent # 6,771,935).

General Comments

My comments are focused on the protection of one's CPNI. Since CPNI includes the telephone numbers called by each customer, this information is extremely personal. The map of telephone numbers that I call is a map of the people that I associate with. Release of this information to the marketplace or to unauthorized governmental entities is highly objectionable and directly impacts the effective functioning of our democracy.

My Data is My Property

My personal data is my personal property. Anyone taking and using this data without my permission is taking my personal property. This applies to both private organizations misusing my personal data and to government entities accessing my data without appropriate court orders.

If I cannot maintain control and dominion over my own personal data (my property) then the future of our democracy is quite limited. This is so because privacy is a necessary component of democracy. One cannot be free in thought and action if one is frequently thinking of how the monitoring organizations are evaluating our thoughts and actions.

This concern applies to specific theft or unauthorized release of my personal data. It also applies to broad monitoring efforts using data mining technology to locate persons of interest.

Removal of Records

As the owner of my data, I must have the right to demand that my data be removed from any and all data bases. This basic right impacts the

Limiting Data Retention aspect discussed in Section 20 (Page 9 of the NPRM). Naturally, I cannot ask a telecommunications company to remove all my data and still receive communications service from that company. However, if I am willing to accept that consequence, I must have the right to request the removal of my data. In practice, most customers will request the removal of their personal data when they drop service by a particular telecommunications company. Some customers will even decide that their privacy is being unduly impacted and they will withdraw from the modern communications environment entirely and depend solely on paper mail.

This basic right can be enforced by charging the telecommunications company rent for retaining the data beyond a basic 30-day compliance period. Make the rent high enough to really hurt over time. I recommend a rent of one dollar for each 100 bytes of data retained for each one-week period of time beyond the 30-day compliance period.

Obtaining Copies of My Data

In order to manage my personal data, I need the right to obtain a print out (or display) of all of my data stored in the organization's data base. This right is absolutely essential and it is provided by current law (Section 4 Page 3 of the NPRM).

Notice

The customer should have the option of being informed each time that a private or governmental organization accesses his or her CPNI. This

notification should include the name of the organization, the physical and/or postal address and phone number of the organization, and a responsible contact person at the organization. The only exception to this rule should be government access conducted under legal and appropriate court orders.

This access notice rule would require the telecommunications companies to maintain a tight control over those allowed access to the CPNI data base. In addition, the companies should be required to control any access to their trunk lines by wiretapping and/or data mining organizations. Organizations can derive CPNI by conducting long-term monitoring of the trunk lines to observe individual call setups and durations.

No Release Orders

Every customer must have the right to issue a no release order for their CPNI. This is consistent with the concept that one's CPNI is one's personal property. This right should not just be restricted to customers who fear stalkers, abusive spouses, or rogue government agents. All property owners (customers) should have the same right to restrict and control their data whatever their reasons for doing so. This is a natural and basic aspect of being a property owner.

Passwords, Audit Trails, and Encryption

Customers should have the option of a security package that would include audit trail tracking and reporting, customer-set passwords, and encryption of the customer's CPNI. Many customers are seriously concerned

about their privacy and these steps would allow them to control their personal data.

Enforcement

Any person, private or governmental, who intentionally accesses CPNI without proper authorization should be jailed for a minimum prison sentence of 10 years without the possibility of parole. This will send the strong message that privacy is a central right in this society and violations of it will not be tolerated. Privacy is essential for our future and even the most powerful public and private organizations must be required to respect it (Refer to Appendix A).

Respectfully submitted,

Nickolaus E. Leggett, N3NL
Amateur Radio Extra Class Licensee
1432 Northgate Square, Apt. 2A
Reston, VA 20190-3748
(703) 709-0752

February 17, 2006

Appendix A – Petition to the FCC on National Security Agency Surveillance

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)
	)
Petition for an Investigation	)
To Determine if Commission	)
Rules are being Violated by	)
Organizations Cooperating with	)
National Security Agency	)
Surveillance of Communications	)
Traffic Conducted Without	)
Court-Ordered Search Warrants	)

To the Commission:

Petition from Nickolaus E. Leggett

The following is a petition from Nickolaus E. Leggett. I am a certified electronics technician (ISCET and NARTE) and an Extra Class amateur radio operator (call sign N3NL). I have a Master of Arts degree in Political Science from the Johns Hopkins University. I am also an inventor holding three U.S. Patents. My latest patent is a wireless bus for digital devices (U.S. Patent # 6,771,935).

This petition requests that the Federal Communications Commission investigate possible violations of the Commission's rules by communications companies and organizations that are cooperating with the National Security Agency (NSA) in the surveillance of telephone calls, emails, and other communications traffic without search warrants from a court. If violations

are found, the Commission is requested to take appropriate enforcement action.

Background

There is widespread press coverage of NSA data mining of civilian communications traffic. This data mining consists of computerized monitoring of communications traffic by means of direct connections to major trunk lines. The monitoring system's software scans the traffic passing through the trunk line looking for identifying data strings and key words to locate potential terrorist communications.

This data mining approach casts a wide net looking for a suspected small set of terrorist communications buried in a huge flood of innocent civilian communications.

Expectation of Privacy

Users of commercial telephone and Internet email communications expect that their communications will be private and will not be examined by the government unless a court has specifically and legally authorized government surveillance. Commission rules support this expectation.

Telecommunications companies are required to cooperate with appropriate court orders for government surveillance of suspect communications. However, cooperating with government surveillance conducted <u>without court orders</u> may directly or indirectly violate the Commission's rules.

Requested Action

I am requesting that the Commission conduct an investigation to determine if communications companies cooperating with the NSA surveillance conducted without court search warrants are violating Commission rules. If violations are occurring, enforcement actions should be taken.

Respectfully submitted,

Nickolaus E. Leggett
1432 Northgate Square, # 2A
Reston, VA 20190-3748
(703) 709-0752

January 24, 2006