Randal S. Milch
Senior Vice President, Legal & External Affairs &
General Counsel
Verizon Business

One Verizon Way
VC43E043
Basking Ridge, NJ 07920

Phone: 908-559-1752
Fax: 908-696-2136
randal.s.milch@verizonbusiness.com

October 12, 2007

The Honorable John D. Dingell
Chairman, Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Edward J. Markey
Chairman, Subcommittee on Telecommunications and
the Internet
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Bart Stupak
Chairman, Subcommittee on Oversight and
Investigations
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairmen Dingell, Markey and Stupak:

Ivan Seidenberg has asked me to respond to your letter to him dated October 2, 2007. I am pleased to be able to provide you with information in response to your questions.

As set out in greater detail below, Verizon has a longstanding and vigorous commitment to protecting its customers' privacy and takes comprehensive steps to protect that privacy. Verizon has safeguards and procedures in place to guard against the improper disclosure or theft of customer information. We review and modify those procedures and policies on a regular basis. Verizon's goal is to minimize the possibility of the improper disclosure of customer information, while at the same time to provide quality service to its customers.

Federal and state laws recognize, however, that criminals and terrorists may use our network to discuss or implement their schemes and explicitly authorize Verizon – through the provisions of the Foreign Intelligence Surveillance Act (FISA) and other statutory provisions – to provide assistance to government entities in their law enforcement and counter-terrorism efforts. Similarly, our business records may be of vital importance in investigations and in emergency situations to protect lives, and existing law authorizes our assistance to government entities in these situations as well.

As you are no doubt aware, as a result of news reports in May 2006, Verizon and other carriers have been the object of numerous class-action lawsuits and a number of state public utility commission investigations relating to alleged assistance with classified counter-terrorism programs allegedly instituted in the wake of the September 11 attacks. In the context of this litigation, we have been informed by the Department of Justice that we cannot confirm or deny Verizon's role (if any) in the alleged programs. *See, e.g.,* Letter from Peter D. Keisler, Asst. Attorney General to John A. Rogovin, Counsel for Verizon, *et al.* at 2 (June 14, 2006). Similarly, the United States has brought suit against Verizon and other carriers, seeking to enjoin Verizon from responding to state public utility commission inquiries prompted by these news reports, because to do so would be "inconsistent with and would violate federal law including, but not limited to, Executive Order 12958, 18 U.S.C. § 798, and 50 U.S.C. § 402 note, as well as other applicable federal laws, regulations, and orders." *See* Complaint, *United States v. Zulima Farber, et. al* at 13 (D.N.J. filed on June 14, 2006).

In light of the Government's position, as most recently reiterated in Ms. Kathleen Turner's letter to Chairman Dingell of today's date, Verizon's responses to your questions herein necessarily exclude any information, discussion, reference to or representations concerning its cooperation, if any, with classified intelligence gathering activities. All of the responses to the numbered questions below are subject to this proviso and must be read consistently with it. I regret that there is any such limitation on our response.

Verizon Wireless was never named in any of the news reports as having allegedly participated in the purported programs (and indeed was dismissed from the litigation mentioned above); these responses are therefore made on behalf of the various wireline operating subsidiaries of Verizon Communications.

1. Please describe the typical process by which your company receives requests for customer records consistent with the FISA process and how such records are disclosed to requesting entities, including how such requests are made, what documents are required, and the timeframe in which your company typically responds.

FISA orders seeking business records are authorized by 50 U.S.C. § 1861. FISA orders are classified documents and as such would be delivered by the government to Verizon personnel holding appropriate security clearances. Pursuant to 50 U.S.C. § 1805(c), FISA orders contain detailed and specific directions relating to the actions

sought and their duration. Given their critical importance to national security, we would comply with such orders as expeditiously as possible.

2. The FISA process permits governmental entities to obtain records, in certain compelling or time-sensitive circumstances, prior to obtaining authorization from the FISA court. In such situations, the government must subsequently seek such authorization within 72 hours of commencing a wiretap or requesting such records. What is the process by which your company complies with such requests? What is the process by which your company assures itself that the requesting entity has subsequently fulfilled its obligation to seek FISA court authorization? How often has your company been requested to commence a wiretap or search for records without an NSL, where the entity seeking such information has subsequently received authorization?

50 U.S.C. § 1805(f) provides for emergency electronic surveillance. In such a situation, and pursuant to those statutory procedures, Verizon would receive a classified written notification that the Attorney General has authorized the emergency surveillance, stating the time of such authorization. We would provide the assistance requested as expeditiously as possible. If we do not receive a FISA order to continue the surveillance within 72 hours of the Attorney General's authorization, the surveillance would be terminated.

A similar procedure is provided for emergency pen register or trap and trace ("pen/trap") requests in 50 U.S.C. § 1843. In these situations Verizon would receive a classified written notification that the Attorney General has authorized the emergency pen/trap, again including the time of such authorization. If a FISA pen/trap order is not received in 48 hours of the emergency authorization, the pen/trap would be terminated.

18 U.S.C. § 2709 authorizes the FBI to issue National Security Letters ("NSLs") for specified customer information or records. That provision does not address wiretaps, and Verizon has not provided assistance to the government to conduct a wiretap based on an NSL.

18 U.S.C. §§ 2702(b)(8) and (c)(4) authorize Verizon to provide the content of stored communications and business records relating to customers to government entities in emergencies, absent a court order or an NSL. Our ability to provide certain information to government entities on an emergency basis is critical to the public safety. Here are some examples:

- Verizon's security teams were able to identify through an IP address the location of a child predator who had abducted a 13 year old girl. Verizon provided the location information to a waiting SWAT team who found the young girl, tied to a bed, but otherwise relatively unharmed. The predator is now serving a 20 year prison term.

- Verizon security working with US Immigration and Customs Enforcement (ICE) agents identified through an IP address the location of a man who was using a webcam to broadcast the sexual abuse of a 6 year old boy. Through Verizon's help law enforcement agents were able to locate and arrest the predator and he is now serving a 30 year prison sentence.

- In April 2007 a New York City Detective sought Verizon's help on an emergency basis in a case involving a gunman holding five hostages. We identified the last working phone service to the address and assisted the NYPD in establishing communications with the hostage taker. The hostages were released uninjured and the gunman was arrested.

- In March 2007, the U.S. Marshals Service was seeking a fugitive charged with holding a gun to the head of a pregnant woman during a home invasion while her child watched. The Marshals learned that the fugitive was armed and using a Verizon DSL line to communicate with associates, and sought Verizon's help on an emergency basis to locate him, using IP subscriber records. His location in Albany N.Y. was established and the Marshals were able to apprehend him without incident.

- In September 2007 the Wood County Schools in Parkersburg, West Virginia were plagued by a series of bomb threats. On September 26, a bomb threat was made to Parkersburg South High School via telephone. Local authorities sought Verizon's help in finding the source of the call on an emergency basis, and two teenagers were arrested the same day.

3. Has your company been asked to produce or provide information relating to your customers without an NSL or FISA authorization? If so, please provide the date or dates such request(s) were made and the form in which such request came. Who or what entity or entities has asked your company to produce or provide information relating to your customers outside of the FISA process?

We have been asked to provide information pertaining to a customer pursuant to federal and state laws other than 18 U.S.C. § 2709 and FISA. There are several federal statutes authorizing the interception of wire and electronic communications (18 U.S.C. § 2510 et seq.); the use of pen/traps (18 U.S.C. § 3121 et seq.); the compulsory production of stored customer communications and records (18 U.S.C. § 2703); and their voluntary disclosure by service providers (18 U.S.C. § 2702). There are similar provisions in various state statutes. We receive thousands of such lawful demands and requests each month.

Because of their volume, I provide here round numbers relating to such requests and demands for the Verizon operating companies for 2005, and for Verizon and the former MCI (jointly) from January 2006 until September 2007. In 2005, Verizon received 90,000 lawful requests and demands for customer information from federal, state and local officials, with approximately 36,000 coming from federal officials, and

54,000 coming from state and local officials. In 2006, Verizon received 88,000 such requests and demands (approximately 34,000 from federal officials and 54,000 from state and local officials), and through September 2007, 61,000 such requests and demands (approximately 24,000 from federal officials and 37,000 from state and local officials). Verizon also received lawful requests for customer information from civil litigants numbering 57,000 in 2005, 69,000 in 2006 and 66,000 through September 2007.

Of the requests and demands coming from federal, state and local officials, requests for emergency assistance were approximately 23,700 in 2005 (240 of which were from federal officials), 25,000 in 2006 (300 of which were from federal officials) and 15,000 through September 2007 (180 of which were from federal officials). Some examples of these emergency responses are set out in my response to Question 2.

Verizon received in 2005 over 1,300 pen/trap court orders, as well as over 250 wiretap court orders requested by federal and state law enforcement authorities. In 2006, we received over 800 pen/trap court orders and nearly 200 wiretap court orders. Through September 2007, these numbers are over 500 and over 130, respectively. These numbers include instances in which wiretap or pen/trap orders were renewed.

4. Did your company raise the lack of FISA process or the lack of an NSL with any entity requesting customer information? If so, what was the governmental entity's response?

In the situations described in response to Question 3, Verizon provided customer information to government entities in reliance on legal authorizations under applicable federal and state laws.

5. What has been the stated legal justification provided by governmental entities for producing or providing information relating to your customers, if any? Do you agree with any stated legal justification provided to you? Did your company conduct any analysis of the legality of a request for customer information? If so, please provide that analysis.

Governmental entities have cited statutory provisions, including those noted in response to Questions 2 and 3, as authorization for production of such information. Because of the complexity of the laws authorizing government requests, however, Verizon on occasion receives requests with incorrect authorizations. For instance, Verizon has received an 18 U.S.C. § 2703(b) subpoena seeking stored voice mail, while 18 U.S.C. § 2703(a) requires a search warrant for that information. Verizon would bring such an error to the attention of the relevant government official and would not respond until an appropriate authorization is received. We do not keep track of these instances; our focus is on having the right authorization for the assistance requested.

6. Do you believe it is proper for the onus to be on a company to determine whether the Government is acting within the scope of its authority when it requests customer information?

No, for a number of important reasons.

Congress has properly enacted a number of protections for telecommunications providers that assist the government. For example, current law states that a telecommunications provider may not be sued for providing assistance to the government, in accordance with the terms of a subpoena, government certification, court order or warrant, among other things. *E.g.,* 18 U.S.C. §§ 2703(e), 2511(2)(a)(ii); 50 U.S.C. § 1805(i). Current law also provides a complete defense to any provider who in good faith relies on a statutory authorization (such as in emergency situations). *E.g.*, 18 U.S.C. §§ 2520(d), 2707(e)(1). If the government advises a private company that a disclosure is authorized by statute, a presumption of regularity attaches. *See Nat'l Archives & Records Admin. v. Favish,* 541 U.S. 157, 174 (2004). Federal statutes also give a provider a complete defense for good faith reliance on other forms of authorization or certain government requests for information. *E.g.,* 18 U.S.C. §§ 2707(e), 2520(d).

These statutory provisions are consistent with longstanding common law principles, which allow citizens to rely on the government's judgment when it asks for assistance. *See, e.g.,* Restatement (Second) of Torts § 139, cmt. d ("To require a person whom a peace officer calls upon to assist in making an arrest to take the risk for being liable in the event that the officer is not himself privileged to make it, unless such person exercises such judgment and makes such investigations as he would be required to make were he acting on his own initiative, would seriously deter such persons from giving the prompt aid necessary to effect arrests which, save in an insignificant minority of cases, the officer is privileged to make.") The person providing assistance is not obligated to second guess the government's stated need for help. *Id.*, cmt. e ("It is for the peace officer and not the actor to determine the necessity for assistance.")

One of the reasons for this rule is that private parties do not have all the information necessary to completely assess the propriety of the government's actions and that such information is uniquely in the control of the government – as for example, how grave and imminent the threat is, how necessary the government's actions are, or whether there are alternative ways of meeting the danger that would be equally effective.

Such an approach is vital to ensuring that providers are able to respond quickly to requests for assistance. Placing the onus on the provider to determine whether the government is acting within the scope of its authority would inevitably slow lawful efforts to protect the public. When an emergency situation arises, prompt assistance is often needed. If the provider were to face legal liability in the event the government is later deemed to have acted outside its authority, the provider would have to meet every request for assistance with extensive questions about the need and justification for the request. The provider would also have to seek legal advice about the merits of the

government's justification. Each of these steps would delay the government's receipt of assistance it might need to save lives.

Moreover, such delays would be unjustified because legal restraints on the government can be used to limit the potential for government abuse. For example, any evidence obtained in violation of the law may be suppressed in any subsequent criminal prosecution. The government also may face legal liability for acting outside its authority. *E.g.,* 18 U.S.C. § 2712.

7. Specifically what information relating to your customers have you been asked to produce or provide outside of the FISA process? What information relating to your customers have you produced or provided to any governmental entities outside of the FISA process?

As stated in response to Questions 2 and 3 above, there are various state and federal laws that govern what types of information and assistance Verizon is required and permitted to provide government entities and private attorneys in civil, criminal and administrative proceedings in addition to the FISA process that cover wiretaps, pen/traps and customer information requests.

Verizon has been asked to provide to government entities "a record or other information," 18 U.S.C. § 2703(c)(1), relating to our customers, including the six categories of information specified in 18 U.S.C. § 2703(c)(2):

1. Subscriber Name;
2. Subscriber Address;
3. Local and long distance telephone connection records, or records of session times and durations;
4. Length of service and type of service utilized;
5. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
6. Means and source of payment for such service, including credit card or bank account number of a subscriber to such service.

We provide records in these categories in response to lawful requests to the extent we maintain them and they are available.

8. Are you currently producing or providing any information to governmental entities outside of the FISA process? If so, specifically what information relating to your customers are you producing or providing outside of the FISA process?

Please see my responses to Questions 3 and 7.

9. Have you at any time sought consent from your customers to produce or provide personally identifiable information to any governmental entities outside of the FISA process?

Verizon has informed its customers that it will respond to authorized government requests for information and will provide information to government entities in public safety situations, so our customers are on notice that we will do so. For example, Verizon's Telephone Company Customer Privacy policy, available on Verizon's website, explains that "we do release customer information without involving you if disclosure is required by law or to protect the safety of customers, employees or property." It further states that "Verizon must disclose information, as necessary, to comply with court orders or subpoenas. Verizon also will share information to protect its rights or property and to protect users of its services and other carriers from fraudulent, abusive or unlawful use of services."

10. What safeguards did you and do you currently have in place to ensure that you do not disclose information relating to your customers in violation of 47 U.S.C. § 222 or any other provision of the Communications Act?

We recognize the importance of protecting our customers' privacy, and customer privacy is a priority for Verizon. Thus, Verizon permits access to Customer Proprietary Network Information (CPNI) to those parties lawfully permitted to have such access, such as Verizon employees acting within the scope of normal business, customers requesting access to their own information, persons designated by the customers, government entities, or Verizon's affiliates or agents, if lawfully permitted. Such access is limited to legitimate business purposes and in compliance with applicable law.

Verizon has a robust security organization and extensive procedures to detect inappropriate access to confidential information. These technical, procedural and organizational measures are designed to safeguard computer systems and detect and thwart unauthorized access to Verizon's databases. Verizon has rigorous measures in place to prevent disclosure of confidential information to any unauthorized party, including "data brokers," private investigators, and Verizon's own employees. Verizon is continually reviewing and updating its security procedures to respond to changes in technology and the evolving tactics of criminals seeking access to CPNI. Because we are concerned that data dealers and others seeking to gain improper access to CPNI could use a detailed technical response to this question as a roadmap for further misconduct, we limit our response here to a summary of some of those safeguards, set forth below.

Employees are trained regarding the privacy protections they are required to undertake to protect sensitive personal information. For example, Verizon employees are trained to follow a strict "Code of Business Conduct," including specific requirements regarding the protection and use of CPNI. Employees who violate company standards and policies may be disciplined up to and including dismissal. Verizon employees' responsibility to safeguard CPNI is also reinforced in the company's methods,

procedures, and refresher training, and compliance is enforced through regular service quality observation. Verizon employees who regularly come into contact with CPNI as a part of their duties are provided additional, specialized training on protecting CPNI. Moreover, Verizon requires responsible senior executives to certify annually that their operations have internal controls in place to comply with Verizon's policies and the statutory and FCC requirements to protect CPNI.

Verizon corporate policy also imposes requirements regarding the proper collection, use and disclosure of sensitive customer information. For example, our policy instructs employees to refrain from displaying sensitive personal information within applications, systems, or databases to individuals who are not authorized to access or view the information and to avoid storing sensitive personal information on removable electronic media unless that media is encrypted. To limit the risk of unauthorized access or fraudulent use of sensitive personal information, all Verizon employees must immediately report any discovery of vulnerability, exposure, loss or unauthorized access to sensitive personal information to Verizon Security.

Each Verizon business unit has a Departmental Compliance Manager who is responsible for developing, implementing, and overseeing CPNI compliance within his or her respective organization. The Departmental Compliance Managers participate in monthly calls to discuss recent developments, legislation, regulatory trends, and business procedures involving CPNI. Members of Verizon's regulatory compliance and legal department also participate in these monthly calls and work with the Departmental Compliance Managers on a regular basis to review issues that may arise and to provide advice and guidance.

Specific caller identity validation procedures are followed prior to discussing account information. In particular, Verizon has procedures in place requiring employees to authenticate customer identity before discussing subscriber account information. These procedures address both employee interactions with residential and business customers over the telephone as well as customer authentication requirements for on-line account management. Verizon consistently evaluates its policies and procedures and changes them as appropriate. For example, as required by new FCC rules, Verizon is changing its policies and procedures to ensure that customers are notified of significant account changes such as a change of address or passwords to give them an opportunity to verify the changes or be made aware of unauthorized access to their accounts. In addition, Verizon has determined that it will no longer discuss call detail information with customers who call in unless the customer provides the specific call to be discussed. General requests to provide call detail information over the phone will be handled by either sending requested information to the address of record or calling the customer back at the account number of record.

Verizon also protects financial information such as customer credit card data in accordance with industry standards, and Verizon's existing operational safeguards are regularly monitored. These include encryption of credit card data while in transit; access controls or masking of data in applications that display credit card information; firewall and intrusion detection systems to protect our internal network and servers; and no

retention of credit card magnetic stripe data, the CVV2 codes (the 3 or 4 digit code on the back of the card), or pin numbers.

11. Have you at any time been offered indemnification for producing or providing information relating to your customers to governmental entities, either within or outside of the FISA process? If so, who or what entity made such offer? Have you at any time been offered compensation for producing or providing information relating to your customers to governmental entities, either within or outside of the FISA process? If so, who or what entity made such offer?

Verizon has not been offered indemnification for the provision of any information to government entities. Congress has, however, consistently required that communications providers be compensated for their costs of responding to lawful requests for information from government entities. For example, Verizon has received compensation for reasonable costs incurred in complying with interception orders pursuant to 18 U.S.C. § 2518(4)(e); for effecting pen/traps pursuant to 18 USC § 3124 (c); for providing stored communications and customer records under 18 U.S.C. § 2706; for providing assistance in effecting electronic surveillance under 50 U.S.C. § 1805(c)(2)(D); and for effecting pen/traps under 50 U.S.C. § 1842(d)(2)(B)(iii).

12. Have you ever been asked to install or permit the installation of equipment on your network to intercept Internet traffic? Have you ever been asked to install or permit the installation of equipment on your network to send copies of Internet traffic to any third parties? If so, who asked you to install such equipment and on what dates? Have you ever installed or permitted the installation of equipment on your network to send copies of Internet traffic to any third parties?

a. Have you at any time been presented with a subpoena or other court or administrative order directing you to install or permit the installation of such equipment? If so, what type(s) of court or administrative order did you receive? On what dates did you receive such subpoenas or other court or administrative orders?

b. If you have ever installed or permitted the installation of equipment on your network to send copies of Internet traffic to any third parties, please identify the third parties to whom copies of Internet traffic were sent.

c. Who asked you to install or permit the installation of such equipment? On what dates did you receive such requests? On what dates did you comply with such requests?

d. What has been the stated legal justification provided by governmental entities for installing or permitting the installation of such equipment and producing or providing such information relating to your customers, if any? Do you agree with any stated legal justification provided to you? Did your company conduct any analysis of the legality of a request to install or

permit the installation of such equipment? If so, please provide that analysis.

e. Have you at any time been offered indemnification for installing or permitting the installation of such equipment and producing or providing such information? If so, who or what entity made such offer? Have you at any time been offered compensation for producing or providing Internet traffic information relating to your customers? If so, who or what entity made such offer?

f. Are you currently producing or providing any Internet traffic information to governmental entities? If so, specifically what information relating to Internet traffic are you producing or providing?

g. Have you at any time sought consent from your customers to produce or provide this Internet traffic information?

The Communications Assistance for Law Enforcement Act ("CALEA") requires telecommunications carriers to ensure that their networks have specified capabilities and capacity related to electronic surveillance. The FCC has determined that CALEA applies to broadband Internet access service. Verizon accordingly has installed equipment and software on its networks to effect CALEA compliance for the interception of broadband Internet traffic.

The various statutes discussed in response to Question 3 each authorize government entities to demand and receive "Internet traffic information." For example, 18 U.S.C. §§ 2510 et seq. and similar state laws permit a demand for Internet traffic including content. 18 U.S.C. § 2703(a) authorizes disclosure of stored email. 18 U.S.C. §§ 2703(c)(1)(B), (2)(C) and (2)(E) permit a lawful demand for information relating to Internet traffic (" session times and durations;" "any temporarily assigned network address"), and 18 U.S.C § 2702(c) authorizes the provision of such information in other defined circumstances, including emergencies. Similarly, 18 U.S.C. § 3127 was modified by the U.S. PATRIOT Act to include "routing" and "addressing" information in the definitions of "pen register" and "trap and trace device." FISA also covers the interception of Internet traffic including content in 50 U.S.C. § 1805 and the use of pen/traps to obtain Internet traffic data in 50 U.S.C. § 1842. Under 50 U.S.C. § 1841, the definitions of pen register and trap and trace device in 18 U.S.C. § 3127 are incorporated into FISA.

Verizon has not been indemnified for meeting its CALEA obligations or in responding to demands under the statutes set out above. As set out in my response to Question 11, however, Verizon has received compensation for its costs consistent with federal law for responding to lawful requests.

The privacy policies discussed in response to Question 9 also cover Verizon's consumer broadband services. In addition, the Verizon Online Privacy Policy informs Verizon Online customers that Verizon discloses information when such "disclosure is

required by law, or deemed necessary by Verizon in its sole discretion to protect the safety, rights or property of Verizon or any other person or entity."

13. On September 9, 2007, the *New York Times* reported that the FBI used NSLs to request not only the call records of particular phone company customers, but also details on those customers' "communities of interest," or the network of people with whom the customers were in contact.

a. Have you at any time been presented with a subpoena or other court or administrative order directing you to produce or provide information about any customer's community of interest? If so, what type(s) of court or administrative order did you receive? On what dates did you receive such subpoenas or other court or administrative orders?

b. Has your company been asked to produce or provide information relating to any customer's community of interest without an NSL or F1SA authorization? If so, please provide the date or dates such request(s) were made and the form in which such request came.

c. What has been the stated legal justification provided by governmental entities for producing or providing such information relating to your customers' communities of interest, if any? Do you agree with any stated legal justification provided to you? Did your company conduct any analysis of the legality of a request for information about your customers' communities of interest? If so, please provide that analysis.

d. Specifically what information relating to your customers' communities of interest have you been asked to produce or provide? What information relating to your customers' communities of interest have you produced or provided to any governmental entities?

e. Have you at any time been offered indemnification for producing or providing information about your customers' communities of interest? If so, who or what entity made such offer? Have you at any time been offered compensation for producing or providing information about your customers' communities of interest? If so, who or what entity made such offer?

f. Are you currently producing or providing any information to governmental entities concerning your customers' communities of interest? If so, specifically what information relating to your customers' communities of interest are you producing or providing?

g. Have you at any time sought consent from your customers to produce or provide information about their communities of interest?

Pursuant 18 U.S.C. § 2703(c)(1), Verizon has received and responded to legal process which asks for information related designated telephone numbers and specific additional information relating to telephone numbers which may have called or been called by the designated numbers.

Verizon has also received subpoenas and NSLs containing "boilerplate" language directing us, for instance, to "Identify a 'calling circle' for the foregoing telephone numbers based on a two-generation community of interest; provide related subscriber information."

Because Verizon does not maintain such "calling circle" records, we have not provided this information in response to these requests; we have not analyzed the legal justification for any such requests, been offered indemnification for any such requests, or sought our customers' consent to respond to such any such requests.

I trust the foregoing information will be helpful to the Committee.

Sincerely,

Randal S. Milch

Randal S. Milch