Klobuchar Questions for the Record

Responses of **Mr. Thomas Dailey**,
Vice President and Deputy General Counsel, Verizon

- *Some experts have expressed concerns that COICA might "break the Internet" by causing more people to use alternative Domain Name System, or DNS, lookup services.*

    - *How long have these alternative systems existed, and do you have any indication that their existence and current usage poses a threat to the Internet?*

      Verizon Response:
      Alternative DNS services have been around for as long as the Internet. DNS is an open system and anyone can operate a DNS server for use by themselves and anyone else anywhere in the world. Historically and today, most DNS services are commodities. It is only recently that entities like Google and Go Daddy have started to try to market differentiated DNS services based on claimed performance or security advantages. Verizon is not aware of any evidence that the existence or use of other equivalent DNS services — that is, services that all provide the same information in response to the same DNS query — threatens the Internet today.

      This said, there are potential issues that could arise if there is a large-scale migration of U.S. Internet users to non-U.S. DNS services.

      1. Network Security Impact. If users leave their ISP's DNS service and migrate particularly to off-shore DNS providers, ISPs will start to lose visibility into DNS queries which can hamper network security efforts. For example, if an ISP can identify DNS queries by bots (malware planted on a user's computer), the ISP can track and potentially thwart a botnet or denial of service attack. This ability would be diminished if customers no longer use their ISP's DNS. In addition, many ISPs employ techniques such as DNS cache-poisoning to help prevent their customers from inadvertently accessing malware and phishing websites. ISPs would lose the ability to help protect their customers from identify theft and other malicious activity for customers who do not use their own ISP's DNS.

      2. National Security Impact. If ISP consumers start using DNS services located outside the U.S., then all of the information generated by DNS query activity would be placed in the hands of foreign DNS providers and/or governments. This also starts to place a subtle operational capability in the hands of non-US companies or governments who could, if they chose to do so, determine which IP address is returned to a US consumer for a particular query. For example, if a computer asks France Telecom where www.whitehouse.gov is located on the Internet (which is what a DNS query does), France Telecom's DNS might not give the same answer as a US-based ISP might provide. This is the more benign case. A more serious situation arises if the foreign DNS provider is not a reputable ISP and instead of returning the correct IP address for www.bankofamerica.com the DNS provider sends the user to a site operated by a

criminal organization by providing an IP address associated with the rogue site, not the real one.

3. Network Performance Issues. A number of commentators have alluded to impacts on Internet performance if U.S. consumers switch to foreign-based DNS providers. These concerns have some merit. As matter of simple physics, DNS queries will take longer if the answers to those queries are based in servers located overseas. Web pages often require multiple (sometimes dozens or more) of individual DNS look-ups to properly load all page content (e.g., images, text, advertisements and so forth), and use of overseas DNS servers will slow this response time. In addition, some content distribution networks make assumptions about end-user location (e.g., East coast versus West coast) based on the IP address of the DNS server the person is using, and try to return geographically-proximate content to end users, which helps speed the delivery of content and provides shorter response times. These assumptions and models will need to change if U.S. consumers change their DNS usage patterns to using DNS services located off-shore.

- *Given that law enforcement would likely issue about 100 court orders per year, are you aware of any evidence that COICA enforcement might cause a massive changeover to alternative domain name systems?*

  Verizon Response:
  The potential for a large-scale abdication of U.S. ISP-provided DNS services will depend on the number of domains actually subject to a blocking order (the fact that the DoJ may only obtain 100 court orders a year does not necessarily mean that only 100 domain names are blocked, since a single court order could involve tens or even hundreds of domain names). Moreover, the longer the blocking remedy is in place, the larger the pool of blocked domain names will become. As the pool grows, public reaction to the blocks may generate a disproportionate number of user defections. Just as importantly, however, the number of U.S. customers who change-over to a foreign-based DNS service also will depend on public perception of and reaction to this new tool in the hands of U.S. government. We simply do not know what the reaction among Internet users will be to government-mandated DNS blocking. Finally, we cannot predict what "work around" solutions people will develop in the future to circumvent the perceived threats posed by COICA. Some have speculated that such services will emerge overseas. If so, this could lead to the adverse consequences described above which would generally be bad for the Internet, even if it does not "break" it.