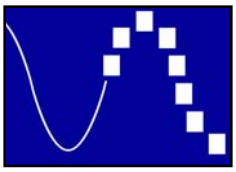
January 31, 2007



EX PARTE

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: Implementation of the Telecommunications Act of 1996: Telecommunication Carrier's Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, RM-11277

Dear Ms. Dortch:

The Voice on the Net ("VON") Coalition supports the Commission's goal of preventing pretexting and protecting confidential customer data against unauthorized release. VON Coalition members have long emphasized the importance of protecting confidential customer data – and already comply with state and federal privacy obligations applicable to providers of on-line data services and to which telecommunications carriers are often exempted. However, we are concerned by proposals to stretch the clear statutory language of Section 222 of the Communications Act of 1934 to apply potentially conflicting obligations on interconnected Voice over Internet Protocol ("VoIP") providers. Imposition of such requirements, especially without an adequate transition period, could thwart the tremendous consumer benefits VoIP brings to Internet and broadband communications.

There are distinct differences between traditional telecommunications and Interconnected VoIP – technologically, legally, and operationally – which have worked to protect VoIP consumers and to thwart pretexters. Technologically, interconnected VoIP providers utilize the latest, up to date, and cutting edge technologies to protect user privacy. Legally, Internet communications fall under a different legal regime; one from which "traditional" telecommunications providers have been exempted. Operationally, VoIP communication utilizes the global Internet, where time and distance are irrelevant, which obviates the need for detailed phone bills containing personal call detail information. These factors have combined to reduce or prevent transmission of customer information of the type that is the core of the Commission's current concerns. In fact, the VON Coalition is not aware of a single case of pretexting involving a VoIP consumer.

I. VoIP Providers Take Seriously Their Responsibility To Protect Consumer Privacy. The VoIP industry is committed to protecting the privacy of customers against "pretexting" and other illicit means of obtaining records and personally identifiable information.

- VoIP providers have implemented a variety of robust privacy safeguards, including many of the safeguards proposed by EPIC (e.g., consumer-set passwords), to protect against unauthorized access to customer information. Internet companies are constantly revising and re-evaluating such procedures to enhance these safeguards and keep a step ahead of the pretexters.

- Companies are using cutting-edge Internet technologies to provide comprehensive privacy protections for their Internet Protocol ("IP")-enabled products. For example, when highly confidential information (such as a credit card number or password) is transmitted over the Internet, companies protect such

information through the use of encryption, such as the secure socket layer ("SSL") protocol common to Internet e-commerce transactions. [1]

- Companies have adopted privacy policies that strictly guard against unauthorized disclosure of sensitive consumer information. These policies are described in detail on company web sites and are available to users 24 hours a day, 365 days a year.[2]

- In addition to these safeguards, the VON Coalition has also published consumer tips for protecting the privacy of billing records for consumers who wish to better protect themselves.[3]

II. New Regulatory Requirements Are Unnecessary Because Internet Companies Are Already Subject to Federal and State Privacy Restrictions.

- VoIP providers are already subject to various federal and state statutes that protect the privacy rights of consumers – privacy laws that often specifically exempt telecommunications carriers.

- The privacy policies that Internet companies have implemented with respect to their products are subject to the jurisdiction of the Federal Trade Commission under Section 5 of the Federal Trade Commission Act ("FTC Act.") Violations are subject to a civil penalty of up to $11,000 per day. The FTC's authority extends to the types of abuses described in the NPRM, including failure by VoIP provider to protect customer information from unauthorized disclosure to data brokers.[4]

- Internet companies must also comply with the Electronic Communications Privacy Act[5], the Children's Online Privacy Protection Act[6], more than 30 state laws that deal with data security,

---

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

[2] *See e.g.,* certification and monitoring services such as TRUSTe <http://www.truste.org/>.

[3] *See* http://www.von.org/usr_files/privacy%20--%20consumer%20tips%20for%20protecting%20data.pdf.

[4] In Congressional testimony, the FTC affirmed that it is strongly committed to investigating companies that engage in pretexting and that it will not hesitate to prosecute "[c]ompanies that have failed to implement reasonable security and safeguard processes for consumer data." Prepared Statement, at 8, of Lydia B. Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission, "Protecting Consumers' Phone Records," Senate Committee on Commerce, Science, and Transportation: Subcommittee on Consumer Affairs, Product Safety, and Insurance (Feb. 8,2006), *available at*: http://commerce.senate.gov/pdf/parnes-020806.pdf.

[5] The Electronic Communications Privacy Act (18 U.S.C. § 2701, *et seq.*) prohibits tampering with computers or accessing certain computerized records without authorization. The Act also prohibits providers of electronic communications services from disclosing the contents of stored communications.

[6] The Children's Online Privacy Protection Act of 1998 (15 U.S.C. §§ 6501 *et seq.*, 16 C.F.R. § 312) requires "verifiable parental consent" before collecting personal information over an online Internet service (but not for telecommunication services) from children under 13 years of age. Sec. 1302(2)(B) specifically exempts entities that are exempt from coverage of Section 5 of the Federal Trade Commission Act.

protection of personal information[7], and breach notification. In many cases, state Internet privacy laws apply only to Internet services and not to telecommunications services.[8]

- There is no need for the Commission to subject VoIP providers to yet another privacy regime that was designed to protect CPNI collected by telecommunications carriers, which are not subject to the FTC's jurisdiction.[9] Doing so would needlessly burden VoIP consumers and providers (contrary to Congress's stated intent),[10] while doing little to enhance consumer privacy.

- Recognizing the global nature of the Internet, the Congress recently enacted and the President recently signed (December 22, 2006) the U.S. SAFE WEB Act of 2006, which further bolsters the FTC's authority to protect consumer privacy and prevent Internet fraud and deception[11] – authority that the FCC lacks under Section 222. In enacting the law, Congress specifically exempted "common carriers."[12]

- In addition, VoIP providers offering services in the European Union already are required to comply with stringent consumer data privacy obligations under the EU's Safe Harbor Privacy Program

---

[7] In 2005, at least 22 states enacted legislation addressing data security breaches that apply to internet data. North Dakota expanded the definition of "personal information" to include mother's maiden name and date of birth. Montana and Arkansas require harm or a likelihood of harm to individuals before notification is mandatory. Several states require notification to nationwide consumer reporting agencies if the number of residents to be notified exceeds a set number (ranging from 500 to 10,000). Many states allow the Attorney General to prosecute violations. Some states require companies to maintain adequate data protection, including destruction procedures.

[8] For example, Nevada Revised Statutes § 205.498 at http://www.leg.state.nv.us/NRS/NRS-205.html#NRS205Sec498 applies only to information services (and not telecommunication services) and prohibits the disclosure of personal information without prior written consent. Likewise, Minnesota Statutes §§ 325M.01 to .09 at http://www.revisor.leg.state.mn.us/revisor/pages/statute/statute_chapter_toc.php?chapter=325M protects personal information for Internet services and specifically exempts telecommunications. In addition, the California Business & Professions Code §§ 22575-22578 at http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579 protects the privacy of online services (not telecommunication services) and requires providers to identify the categories of personally identifiable information collected about consumers who use online services and third parties with whom the operator may share the information.

[9] 15 U.S.C. 5 45(a)(2). Because telecommunications carriers are not subject to the FTC's jurisdiction, their privacy practices are, by necessity, overseen primarily by the FCC pursuant to Section 222 of the Act, while the privacy practices of information service providers and other firms are regulated by the FTC. *See* Letter from Deborah Platt Majoras, Chairman, FTC, to Hon. F. James Sensenbrenner, Jr., Chairman, Committee on the Judiciary, U. S . House of Representatives, at 3 (April 14, 2006) ("The FTC is the only federal agency with general jurisdiction over consumer protection and competition in most sectors of the economy, including broadband Internet access services.").

[10] *See* discussion *infra* Section II.D.

[11] Undertaking Spam, Spyware and Fraud Enforcement With Enforcers Beyond Borders Act of 2006, Pub. L. No. 109-455. The law confirms the FTC's authority to redress domestic harm caused by foreign wrongdoers and vice versa and extends existing remedies to cross-border cases.

[12] Sec. 4(j)(6) limiting the FTC's authority to take action with respect to common carriers.

Requirements. In many cases, impacted providers extend these safeguards worldwide, including to their U.S. customers.[13]

- Nothing in the record indicates that the Internet privacy protection authority that Congress has vested with the FTC, and the myriad other state statutes that have been enacted to protect Internet privacy have been insufficient to protect the privacy of VoIP users. Moreover, the FCC has not investigated whether the privacy rights of Internet users would actually be *weakened* by applying potentially contradictory obligations.

III. VoIP Can Be A Part of a Pretexting Solution

- Internet voice services that transcend LATA boundaries often have no reason to charge more for long distance calls, and thus there is often no need to expose detailed information in phone bills. As EPIC pointed out in testimony before Congress –as more people switch to VoIP, pretexting problems may simply "disappear"[14] because many VoIP services are offered as flat rate services. With flat rate services, there is no need to include call detail information for who you called, how long the call lasted, whether you have exceeded your minutes, and whether it was a local or long distance call. Privacy experts warn that forcing companies to collect more information – as other proposals before the commission would appears to require[15] – could actually increase the privacy problems and the likelihood that private information could be misused.

- The faster America can transition to VoIP services, the quicker America can rid itself of one of the key features that is driving the scourge of pretexters – the need for phone bills riddled with private call detail information. At the same time, the VON Coalition agrees with Chairman Martin's statements that the Commission should exercise regulatory restraint where there is not significant evidence of real problems.[16] Adding new and potentially conflicting rules, where there isn't a sign of a problem and where the Commission's statutory authority is in question, could slow the roll out of the very type of services that can be beneficial in thwarting pretexting.

IV. VoIP Offerings Have Not Been Classified As "Telecommunications Services," and, Therefore, Are Not Subject to Section 222 of the Communications Act.

- Section 222 of the Communications Act specifically applies to "telecommunications carriers" and the CPNI the "carrier" receives "by virtue of its provision of telecommunications services." [17]

---

[13] Under the Safe Harbor guidelines, companies must self-certify compliance with privacy requirements regarding the collection, use, and retention of personal data from the EU. *See* US. Department of Commerce, "Introduction to the Safe Harbor" *available at* http://www.export.gov/safeharbor.

[14] Marc Rotenberg, Electronic Privacy Information Center, Feb. 8, 2006, US Senate hearing indicated that as more phone services switch to flat rate billing as happens with VoIP, "many of the threats to privacy would simply disappear."

[15] Phantom Traffic requirements, as the VON Coalition has told the Commission previously, would apply per-minute access charges to these services and potentially end the kind of flat-rate offerings that thwart a pretexter's ability to discover call details.

[16] FCC Chairman Kevin Martin, Reuters 12/27/05: "I'm hesitant to adopt rules that would prevent anti-competitive behavior where there hasn't been significant evidence of a problem," and "...there's a significant difference between potential problems and problems that occur."

[17] 47 U.S.C. §222.

- The FCC has not declared interconnected VoIP or other types of end-user VoIP services to be "telecommunications services" provided by "telecommunications carriers".

- The bases for extension of other regulations to interconnected VoIP services do not exist here (e.g., there is no alternate statutory definition as in CALEA, there is no permissive authority for "providers of telecommunications" as in Section 254 and Universal Service).[18]

- Many VoIP applications are explicitly information services and, consequently, are not subject to the requirements of Section 222 that only apply to "telecommunications carriers" and "telecommunications services."[19]

- To the extent the FCC proceeds to apply it to VOIP, section 222 should only apply to VoIP services that enable users to make and receive calls and that are a direct substitute for telephone service**.** Not all VoIP services that touch the PSTN should be subject to the FCC's CPNI rules. Specifically, the FCC should only apply its CPNI rules to interconnected VoIP services that enable users to ***make and receive*** phone calls to and from the PSTN and are ***sold and marketed*** as substitutes for traditional phone service. This is because not all PSTN interconnected VoIP services allow users to ***make and receive*** calls, but rather connect to the PSTN for purposes of facilitating another service. An example is a web-based VoIP conferencing service where a consumer may purchase a PSTN bridge from a carrier in order to access a PC-based web conference session. So, the web conferencing provider does not market its service as a substitute for traditional telephone service, the service does not offer users an ability to make and receive calls, but since its service connects to the PSTN (via the bridge), it could be construed to fall under the Commission's definition of interconnected VoIP. These IP-based services are not phone substitutes and should not be subject to legacy carrier CPNI rules.

V. Courts Have Strictly Limited the Commission's Authority Under Title I of the Act to Impose Title II Obligations on Non-Carriers.

- The Microsoft, Skype, and Yahoo filing of April 28, 2006 in this docket explains why the Commission lacks subject matter jurisdiction under Title I to regulate a VoIP provider's post-transmission practices regarding sensitive customer information. Certain of the potential new obligations that have been suggested - e.g., deleting or encrypting stored sensitive customer data, maintaining "audit trails" regarding the disclosure of such data, and post-transmission breach notice requirements - would appear to seek to regulate practices that occur entirely after a VoIP call has terminated.

---

[18] *See American Council on Education v. FCC*, 451 F.3d 226 (D.C. Cir. 2006) (interconnected VoIP subject to CALEA based upon statutory definition of "telecommunications service" broader than the definition contained in the Communications Act); *Universal Service Contribution Methodology,* Report and Order and Notice of Proposed Rulemaking, 21 FCC Rcd 7518 (2006)(appeal pending)(subjecting interconnected VoIP providers to the Universal Service contribution scheme by virtue of Section 254(d) permissive authority over any "other provider of interstate telecommunications").

[19] The FCC has held repeatedly that information services are not Title II services. *See, e.g.,* 47 C.F.R. § 64.702(a); *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 14853, ¶108 (2005) ("Title II obligations have never generally applied to information services, including Internet access services.") (citing precedents). However an information service provider's privacy policies applicable to those products would be subject to the jurisdiction of the FTC, as are the privacy policies of most commercial firms.

- If the Commission determines that it has the statutory authority to extend the clear language of Section 222 to interconnected VoIP providers, it should make clear that CPNI rules do not extend to non-interconnected VoIP services when offered as standalone services or where a non-interconnected VOIP service is offered in conjunction with an interconnected VOIP service. Specifically, the FCC should only apply its CPNI rules to "interconnected VoIP services" that enable users to ***make and receive*** phone calls to and from the PSTN and are sold and marketed as substitutes for traditional phone services. Where there is a bundled offering, only the interconnected-VoIP service portion of the offering should be subject to the Commission's CPNI rules. For example, carriers' CPNI obligations under the Communications Act should not apply to the peer-to peer VoIP, e-mail, or instant messaging features of an interconnected VoIP service provider's offerings. For such non-telecommunications services, the FTC already has authority to protect consumers' privacy to apply to the computer data associated with a software application that integrates voice into data functions and performs other functions beyond mere PSTN connectivity and voice communication – such as voice xml applications -- under Section 5 of the FTC Act.

VI. Extending the FCC's CPNI Rules to VoIP Providers at This Time Is Unnecessary, and Would Likely Be Counterproductive, Costly, and Frustrating for Consumers.

Rather than immediately extending the Title II CPNI rules to Internet services, where there is no evidence of a problem and there exists significant question regarding the Commissions legal authority to do so, the Commission should instead develop a full and complete record by opening a Further Notice of Proposed Rulemaking. An FNPRM could address for example, the jurisdictional issues between the Commission and the FTC, how various state and federal statutes would be harmonized, how the traditional telecommunications rules and requirements practically translate into the IP world, and how converged data applications should be handled. Such action could be taken without in any way harming consumer privacy in the interim, which, as we have explained above, is already protected.

However, if the Commission does decide to apply CPNI rules to Interconnected VoIP providers without a FNPRM, the Commission must give providers sufficient time to transition their systems to meet any new requirements and to sort through potentially conflicting legal regimes. The Commission has previously allowed *more than a year* for telecommunications providers to come into compliance with its CPNI regulations. More specifically, in February 1998, when the Commission released its initial rules implementing Section 222, it gave providers 11 months to implement the rules "[b]ecause the Commission anticipated that carriers would need time to conform their data systems and operations to comply with the software flags and electronic audit mechanisms required by the Order." In September 1998, recognizing "that it will take time and effort to implement these requirements," the Commission extended the compliance timeframe by another 6 months. Ultimately the Commission gave providers more than two years to implement the software flag and electronic audit mechanisms required by the original Section 222 rules.

We understand that the Commission is considering requiring interconnected VoIP providers to comply with the legacy CPNI rules *upon publication in the Federal Register*.[20] We have found nothing in the record that suggests that Interconnected VoIP providers should or could comply in this extraordinary timeframe, while it took others more than 2 years to comply. Imposing such an onerous implementation timeframe on VoIP providers is especially disconcerting, considering that VoIP providers would simultaneously have to implement whatever updated rules the Commission adopts on a separate timetable and, seek consistency between federal and state privacy statutes, and modify various contracts to reflect new requirements. Customer confusion should be minimized by allowing for only one harmonized transition timetable. The Commission is also aware that, at the same time these CPNI requirements would

[20] Per Section 1.427 of the Commission's rules, 47 C.F.R. § 1.427, rules are generally effective 30 days *after* publication in the *Federal Register*.

be added, many VoIP providers will be making their first FCC Form 499A filings and working towards compliance with the Commission's CALEA implementation deadlines.

The Commission should not adopt two separate compliance timetables for Interconnected VoIP providers. Instead, it should place compliance with any legacy rules on the same timetable as compliance with any new rules, and it should ensure that the transition timeframe is reasonable. The VON Coalition agrees with USTelecom's suggestion that one year would be a reasonable period of time for carriers to implement any new CPNI rules.

Sincerely,

The VON Coalition