

May 17, 2006

Chairman Kevin Martin  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, DC 20554

Dear Chairman Martin:

We are writing to you regarding privacy protection for American telephone customers and the growing public concern that American telephone companies, subject to FCC regulation, have improperly released call detail information to the National Security Agency.

EPIC has worked closely with the Commission over the past year to establish stronger safeguards for call record information. We brought the problem of call records sales to the attention of the FCC last year,<sup>1</sup> and we support the Commission's recent rulemaking on this issue that we hope will establish stronger security standards for customer information maintained by the telephone companies.<sup>2</sup> We share your concern that "[t]he disclosure of consumers' private calling records is a significant privacy invasion."<sup>3</sup>

Now we write to urge you to undertake an investigation of the various reports that customer information was improperly disclosed to the National Security Agency. We appreciate that there are circumstances under which the government may properly obtain customer information from the telephone companies. But it is vital that such disclosures are undertaken pursuant to legal authority. If telecommunications carriers disclosed customer information to the NSA in the manner described in press reports, then violations of section 222 of the Communications Act have occurred.

The accounts that have been provided by some of the phone companies regarding their involvement in the NSA program have hardly resolved the matter. For example,

---

<sup>1</sup> Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005).

<sup>2</sup> See, e.g., Comments of the Electronic Privacy Information Center *et al.* on the petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network information, CC Docket No. 96-115 (filed Apr. 14, 2006).

<sup>3</sup> *Ban needed on sale of private phone records, lawmakers told*, Associated Press, (Feb. 1, 2006), [http://energycommerce.house.gov/108/News/02012006\\_1768.htm](http://energycommerce.house.gov/108/News/02012006_1768.htm).

Verizon issued a statement on May 12, 2006 in which it said that “Verizon does not, and will not, provide any government agency unfettered access to our customer records or provide information to the government under circumstances that would allow a fishing expedition,” but it did not explicitly state that it had not provided customer record information to the National Security Agency.<sup>4</sup> The press release issued on May 16, 2006 says that the company did not provide customer phone records to the NSA from certain businesses under the control of Verizon, but also leaves open the question of other means by which the company may have provided customer information to the agency.<sup>5</sup>

The May 12 statement from Verizon is also significant regarding the possible participation of MCI, a company acquired by Verizon, in the NSA program. Verizon said in the press release, “In January 2006, Verizon acquired MCI, and we are ensuring that Verizon’s policies are implemented at that entity and that all its activities fully comply with law.” However, Verizon provided no indication of whether MCI had disclosed customer record information to the NSA prior to January 2006. Moreover, even the May 16, 2006 statement from the company leaves open the question of whether customer record information in the possession of Verizon was provided to the National Security Agency.

The statement from BellSouth also raises troubling concerns. The May 15 statement from the company stated, “based on our review to date, we have confirmed no such contract exists and we have not provided bulk customer calling records to the NSA”<sup>6</sup> (emphasis added). The use of the word “contract” in this context, coupled with a news report on the same matter, suggests that the telephone companies may have actually sold customer record information to the government.

With more questions being raised each day about the scope of participation by the telephone companies in the NSA’s domestic surveillance program, the need for the FCC to undertake a comprehensive investigation has become clear.

Privacy protections have long been central to the provision of communications services in the United States. Section 605 of the original Communications Act of 1934 established a clear prohibition on the use of information obtained by wiretapping in a criminal proceeding. Section 222 of the amended Act makes clear that telecommunications companies have an ongoing obligation to protect the confidentiality of customer proprietary network information.

---

<sup>4</sup> Press Release, Verizon, Verizon Issues Statement on NSA and Privacy Protection (May 12, 2006), <http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93446>

<sup>5</sup> Press Release, Verizon, Verizon Issues Statement on NSA Media Coverage (May 16, 2006), <http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93450>

<sup>6</sup> Press Release, Bell South, BellSouth Statement on Governmental Data Collection, (May 15, 2006), [http://bellsouth.mediaroom.com/index.php?s=press\\_releases&item=2860](http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860)

The Commission plays a critical role in safeguarding the privacy of American consumers. We look forward to hearing from you as soon as possible regarding the action the FCC intends to take.

Sincerely,

Marc Rotenberg  
EPIC Executive Director

Lillie Coney  
EPIC Associate Director

Sherwin Siy  
EPIC Staff Counsel