February 5, 2007

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
12th Street Lobby, TW-A325
Washington, D.C. 20554

Re: FCC CC Docket No. 96-115: CPNI Notice Requirements

Dear Ms. Dortch:

I am writing on behalf of CTIA - The Wireless Association® ("CTIA") regarding the recently filed Department of Justice *ex parte* proposal in the above-captioned proceeding that would require telecommunications carriers to notify the Federal Bureau of Investigation and the U.S. Secret Service in the event of any breach of security resulting in the unauthorized use, disclosure or access to customer proprietary network information ("CPNI"). This proposal was first described in Deputy Attorney General Paul McNulty's December 28, 2006 letter to the Commission.

The proposal, if adopted by the FCC in the manner proposed by the Department, inadvertently could require carriers to report immaterial breaches and could force carriers to delay notifying customers of major security breaches. Both of these elements could create a direct conflict with certain state security breach notification laws. We have contacted the Department of Justice and conveyed our concerns regarding the breadth of the proposal, as well as its conflict with state laws. CTIA asks the Commission to delay any final action on the Department's proposal until we have had an opportunity to address our concerns with the Department. In addition, CTIA asks the Commission to seek comment on the notion of a materiality standard for reporting information breaches.

CTIA's members take seriously their obligation to protect their customers' CPNI. In addition, we share the Department's interest in seeing the prosecution of those who attempt to steal or misuse CPNI, and we certainly share the goal of ensuring that criminal investigations and national security are not compromised in the notification process. Indeed, to that end, wireless carriers already are complying with state security breach notification laws that have the same purpose as the new requirements being proposed by the Department.

Thirty-four states have security breach notification laws that require carriers to promptly notify customers, credit reporting agencies and state and local authorities in a variety of ways. However, contrary to the Department's proposal, none of the state laws currently mandate automatic delayed notice to customers once a breach is discovered, although all but one permit notice to be delayed at the request of law enforcement. The Illinois breach notification law is particularly problematic because it does not contain a provision for delayed notice, stating that

"disclosure notification shall be made in the most expedient time possible and without reasonable delay." 815 Ill. Comp. Stat. 530/10(a) (emphasis added).

CTIA is concerned about the creation of federal compliance obligations without addressing conflicts with state law. Regardless of the merits of the underlying claim, with conflicting federal and state mandates, a party aggrieved by a violation of state disclosure law – in this case a person injured by the delay in learning that his or her CPNI was wrongfully disclosed – could bring a third-party enforcement action against the provider that delayed such notice. Moreover, state consumer protection agencies also can bring enforcement actions against providers who disregard state mandates. Rather than engage in litigation to resolve how a carrier should attempt to comply with federal obligations that conflict with state disclosure notification laws, we believe the Department and the Commission should address and resolve these conflicts ex ante by reviewing and revising the Department's proposal to either clearly preempt conflicting state security breach laws, or more narrowly tailor the federal requirements.

The Department's proposal also requires that all breaches be reported to the U.S. Secret Service and the FBI -- unlike state laws, which generally target only breaches of electronic networks or computerized data. While the Department is in the best position to determine the most appropriate use of its investigative resources, it would seem that the Department's interests would be better served by a standard that requires carriers to only report the most significant breaches. We urge the Commission to adopt a more narrow definition of breach so that the reporting impact on carriers, and the information received by federal law enforcement, can be limited to incidents of reasonable significance.

We think it is important for the Commission to seek comment on the notion of a materiality standard for reporting information breaches. North Carolina, for example, requires notification to the Consumer Protection Division of the state Attorney General's office only if a company provides notice of a breach to more than 1,000 persons at a time. A targeted further notice also would permit more detailed consideration of how the Justice Department's proposal would interact with the requirements of the Telephone Records Privacy Protection Act, which the President signed into law on January 12, 2007. As you know, this Act criminalizes pretexting and related activities and will change the landscape by drying up the demand for telephone records. A further notice also would help clarify the extent of any potential conflict between this proposal and the provisions of the Electronic Communications Privacy Act that govern the legal process needed for disclosure to governmental entities of records concerning electronic communication service or remote computing service.

For the foregoing reasons, CTIA requests that the Commission briefly delay any final action on the Department's proposal and seek comment, through a Further Notice, on the issue addressed above. Pursuant to Section 1.1206 of the Commission's Rules, this letter is being electronically filed with your office. If you have any questions concerning this submission, please contact the undersigned.

Sincerely,

/s/ Christopher Guttman-McCabe

Christopher Guttman-McCabe