

January 25, 2007

Writer's Direct Contact
202/887-1574
WMaher@mofocom

Via Electronic Filing

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

Re: **EX PARTE NOTICE** - Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information - CC Docket No. 96-115, RM-11277

Dear Ms. Dortch:

On January 25, 2007, Tom Sugrue, Kathleen Ham, and Sara Leibman of T-Mobile USA, Inc. ("T-Mobile") and the undersigned, on behalf of T-Mobile, met with John Branscome of Commissioner Copps' office regarding the above-referenced proceeding. The T-Mobile representatives explained T-Mobile's positions on potential new regulations of customer proprietary network information ("CPNI"). As discussed below, these positions are consistent with T-Mobile's prior filings in this proceeding, including its comments and reply comments and its ex parte filings.

Call-In Access to Customer Service. T-Mobile representatives do not disclose call detail records over the phone, and customer-set passcodes are optional for call-in access. Any new rules should permit T-Mobile to continue this arrangement, with flexibility for T-Mobile representatives to discuss with authenticated customers issues about their bills. "Call detail records" should be defined narrowly, to focus on the phone numbers and locations associated with a caller, which are the pieces of information of most interest to pretexters.

On-Line Access. T-Mobile requires customer-set passcodes for on-line access to customer information. The Commission should not adopt rules that would require T-Mobile to police the content of passcodes that its customers set. T-Mobile customers appropriately control the content of their passcodes.

Customers establish on-line access through the registration page of My T-Mobile.com, where they enter their mobile phone number. T-Mobile immediately sends a random temporary

Marlene H. Dortch
January 25, 2007
Page Two

password to the customer's handset by text message. The customer then goes to the next screen on My T-Mobile.com and is prompted to enter this temporary password. The customer then must provide their first and last name and e-mail address. Finally, the customer must change the temporary password, and the newly created password must be entered twice for confirmation. T-Mobile customers with on-line access through My T-Mobile.com are able to change their passwords at any time.

Coordination with Law Enforcement. T-Mobile is concerned about the rule proposed by the U.S Department of Justice on December 28, 2006 (the "DOJ proposal") that would require carriers to notify the Federal Bureau of Investigation ("FBI") and the U.S. Secret Service ("USSS") of CPNI breaches prior to those carriers notifying their customers.¹ T-Mobile strongly supports the efforts of law enforcement agencies to apprehend pretexters and protect carriers and consumers. However, T-Mobile urges the Commission to release a targeted further notice of proposed rulemaking ("further notice") on the DOJ proposal. Public comment on the DOJ proposal would yield valuable input to the Commission about its feasibility and the potential burdens it could place on carriers, their customers, and federal law enforcement agencies themselves.

T-Mobile notes, for example, that the DOJ breach notification proposal would require carriers to notify the FBI and the USSS of *any* unauthorized use, disclosure, or access to CPNI. T-Mobile believes that this broad notification and record-keeping requirement will be overly inclusive and potentially very burdensome without some reasonable narrowing, as AT&T has suggested.² T-Mobile is concerned that in the DOJ proposal, the event that starts the clock on the notification obligation – a carrier's "reasonable determination of the breach" – is ambiguous, and suggests that "actual knowledge of a breach" by a carrier may be a more reliable event.

T-Mobile also believes that a further notice is necessary to develop a record on the DOJ proposal's relationship with existing state laws that address security breaches. Only a handful of states (e.g., Hawaii, Louisiana, Maine, New Hampshire, New Jersey, New York, North Carolina, and Vermont) require various types of companies to notify state law enforcement officials or regulators of such breaches under a variety of circumstances.³

¹ See Letter from Paul J. McNulty, Deputy Attorney General, U.S. Department of Justice, to Kevin J. Martin, Chairman, Federal Communications Commission, CC Docket No. 96-115 (Dec. 28, 2006).

² See Letter from Anisa A. Latif, AT&T, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 (Jan. 17, 2007) (proposing that carriers only be required to notify law enforcement of "material fraudulent access" to customer accounts).

³ See HAW. REV. STAT. § 487N-2 (2006); LA. REV. STAT. ANN. §§ 3071 *et seq.* (2006); ME. REV. STAT. ANN. tit. 10, §§ 1346 *et seq.* (2006); N.H. REV. STAT. ANN. § 359-C:20 (2006); N.J. STAT. ANN. § 56:8-163 (2007);

Marlene H. Dortch
January 25, 2007
Page Three

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.⁴ Only one state requires notification of a security breach to a law enforcement agency before notifying the customer.⁵

Public comment on a targeted further notice would permit more detailed consideration of how the DOJ proposal would interact with the requirements of the Telephone Records Privacy Protection Act, which the President signed on January 12, 2007 and which criminalizes pretexting and related activities. 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.⁶

Opt-In Customer Approval and Total Service Approach. T-Mobile agrees with Verizon that the FCC should not adopt an opt-in rule that would require carriers to obtain customer consent before sharing customer information with independent contractors and joint venture partners.⁷ Such a rule is unnecessary and would not address the pretexting problem. As Verizon explains, the types of information shared with third party marketing firms is not of interest to pretexters and there is no indication in the record that pretexters are obtaining call detail information from independent contractors.⁸

Moreover, the Commission should retain its total service approach to CPNI by leaving unaltered the current operation of section 64.2005 of the Rules.⁹ The Commission derived

N.Y. GEN. BUS. LAW § 899-aa; N.C. GEN. STAT. § 75-65 (2006); and VT. STAT. ANN. tit. 9, § 2435 (2006). Each law differs in multiple respects.

⁴ See N.C. GEN. STAT. § 75-65(f) (2006).

⁵ See N.J. STAT. ANN. § 56:8-163 (2007).

⁶ See, e.g., 18 U.S.C. § 2703(c).

⁷ See Letter from Donna M. Epps, Verizon, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115, RM 11277 (Jan. 18, 2007) (discussing "independent contractors that assist carriers in their marketing efforts").

⁸ See *id.* at 1-2.

⁹ See 47 C.F.R. § 64.2005(a) ("Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval."). See also 47 C.F.R. § 64.2005(b)(1) ("A wireless provider may use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s).").

Marlene H. Dortch
January 25, 2007
Page Four

the total service approach for all carriers from Section 222(c)(1) of the Communications Act¹⁰ and that approach has permitted carriers to efficiently offer new and innovative services to their customers.¹¹ There is no basis from a legal or policy perspective for the Commission to graft onto this rule a customer approval requirement.

Notification of Passcode Changes. T-Mobile notes that it is important for carriers to have flexibility in the form and means of notifying customers of password changes, and that such means should include text messaging (SMS).

Implementation Deadlines. The Commission should permit a reasonable time to implement those portions of any new or modified CPNI rules that would require changes to carrier systems or notice to customers, especially changes affecting call-in access, on-line access, the DOJ proposal, existing opt-out requirements, and notifications of password changes. T-Mobile has supported a twelve-month implementation period and continues to believe that such a period is reasonable.

Pursuant to Section 1.1206 of the Commission's rules, an electronic copy of this letter is being filed with the office of the Secretary. If you have any questions regarding this notification, please contact the undersigned.

Very truly yours,

/s/ William F. Maher, Jr.
William F. Maher, Jr.
Counsel for T-Mobile USA, Inc.

cc: John Branscome
Michelle Carey
Ian Dillner
Barry Ohlson
Scott Bergmann
John Hunter
Angela Giancarlo
dc-476032

¹⁰ See 47 U.S.C. § 222(c)(1) (“...a telecommunications carrier that receives or obtains [CPNI] shall only use, disclose or permit access to individually identifiable [CPNI] in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications services....”).

¹¹ In establishing the total service approach, the Commission properly recognized differences between CMRS and wireline carriers. See, e.g., 47 C.F.R. § 64.2005(b)(1).