

BEFORE THE  
Federal Communications Commission  
WASHINGTON, D.C.

|   |   |                      |
|---|---|----------------------|
| In the Matter of  | ) |                      |
|   | ) |                      |
| Implementation of the Telecommunications Act of 1996;   | ) | CC Docket No. 96-115 |
|   | ) |                      |
| Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information;                    | ) |                      |
|   | ) |                      |
| Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information | ) | RM-11277             |
|   | ) |                      |
|   | ) |                      |

**COMMENTS OF TIME WARNER TELECOM**

Willkie Farr & Gallagher LLP  
1875 K Street, N.W.  
Washington, DC 20006  
(202) 303-1000

ATTORNEYS FOR TIME WARNER TELECOM

April 28, 2006

BEFORE THE  
Federal Communications Commission  
WASHINGTON, D.C.

|   |   |                      |
|---|---|----------------------|
| In the Matter of  | ) |                      |
|   | ) |                      |
| Implementation of the Telecommunications Act of 1996;   | ) | CC Docket No. 96-115 |
|   | ) |                      |
| Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information;                    | ) |                      |
|   | ) |                      |
| Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information | ) | RM-11277             |
|   | ) |                      |

**COMMENTS OF TIME WARNER TELECOM**

Time Warner Telecom Inc. ("TWTC"), by its attorneys, hereby submits these comments in response to the FCC's Notice of Proposed Rulemaking in the above-captioned proceeding.<sup>1</sup> The purpose of that NPRM is primarily to address issues covered in a previously filed petition for rulemaking filed by the Electronic Privacy Information Center ("EPIC")<sup>2</sup> regarding possible changes to the FCC's customer proprietary network information ("CPNI") rules.

**I. INTRODUCTION AND SUMMARY**

The *CPNI NPRM* reflects a justified concern with the problem of pretexting, the practice of impersonating a customer for the purpose of obtaining the customer's CPNI from his or her

---

<sup>1</sup> See *Implementation of the Telecommunications Act of 1996, et al.*, Notice of Proposed Rulemaking, 21 FCC Rcd 1782 (2006) ("*CPNI NPRM*").

<sup>2</sup> Electronic Privacy Information Center, Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Dkt. No. 96-115 (filed Aug. 30, 2005) ("*EPIC Petition*").

carrier and subsequently selling access to such CPNI. There should be no dispute that this practice should be forbidden. The only real question is how best to implement and enforce such a prohibition. Three basic principles should guide this inquiry.

*First*, the Commission should avoid adopting any rules designed to address pretexting while there is a realistic prospect, as there is now, of federal legislation addressing this issue. Otherwise, the Commission would run the risk of adopting rules requiring costly carrier implementation and compliance only to have such rules superseded or rendered unnecessary by subsequently adopted legislation.

*Second*, any federal regulations that are ultimately adopted to prevent pretexting should be narrowly targeted to address pretexting itself and to avoid the imposition of unnecessary and ineffective regulation. The proposals discussed in the *CPNI NPRM* would do little, if anything to prevent pretexting. Those proposals' most fundamental flaw is that they would impose regulation on carriers. But carriers have powerful incentives to protect their customers' data, because customers are less likely to subscribe to service from a carrier that fails to protect its customers' CPNI and because the CPNI of a carrier's customers is a critically important tool for identifying additional selling opportunities. In any event, Sections 222(a) and (c) of the Communications Act already impose comprehensive obligations upon carriers to ensure the confidentiality of CPNI.

Rather than impose unneeded and ineffective regulation on carriers, government resources should be targeted at prosecuting the pretexters themselves under existing law. Indeed, such lawsuits (as well as those brought by carriers) are ongoing. In light of this aggressive enforcement environment, it is likely that pretexters will soon find it difficult to do business.

*Third*, even if the FCC were to adopt pretexting regulations applicable to carriers, it should not apply the same level of regulation to all carriers. Rather, the Commission should account for the types of customers a carrier serves and the size of the carrier when determining whether and to what extent new regulations should apply to a particular class of carriers. For example, the FCC should not apply any new rules addressing pretexting to small carriers, such as TWTC, that serve exclusively enterprise and wholesale customers. This is because the available evidence indicates that pretexting primarily or exclusively affects mass market customers and the carriers that serve mass market customers. It cannot be that large compliance costs outweigh the benefits for small carriers serving only enterprise customers.

## **II. DISCUSSION**

There should be no debate that the pretexting practices that prompted the *EPIC Petition* and the *CPNI NPRM* must be eliminated to the extent possible. Pretexting results in inexcusable violations of individuals' privacy. It also threatens to undermine customers' trust in the systems carefully designed by carriers to protect customer information. Such customer concerns can reduce their willingness to share information with or to allow carriers legitimate access to CPNI. If this were to occur, carriers would have a reduced ability to offer efficient communications solutions to their customers and consumer welfare would be harmed.

The real issue in this proceeding is how best to address this important problem, and specifically whether increased regulation of carriers within the FCC's jurisdiction is the appropriate approach at this time. As explained herein, this is not the approach that the federal government should adopt, especially with regard to smaller carriers and carriers that serve exclusively the enterprise market.

*First*, the Commission should not take any action while there is a significant chance that Congress will pass legislation addressing pretexting. It is important that the FCC not implement

regulations that either conflict with new federal legislation or that would impose expensive and burdensome requirements on carriers that may soon be superseded by new statutory directives. If this were to occur, carriers would be required to revamp their systems and change their practices to comply with FCC requirements only to scrap some or all of those new systems and processes in favor of systems and processes required by the new legislation. Similarly, it is entirely possible that Congress will adopt legislation that fully addresses the pretexting problem in ways that obviate the need for any federal agency to adopt regulations addressing the issue.

The pretexting bills pending before Congress could lead to either of these outcomes. For example, one of the bills introduced in Congress to address pretexting, the Consumer Telephone Record Protection Act of 2006 (S. 2389), would alter the current CPNI rules and mandate specific CPNI safeguards. Among other things, that bill requires that the FCC create safeguards that are “similar in scope and structure” to the “safeguards rule” promulgated by the FTC to enforce the Graham-Leach-Bliley Act regulations regarding privacy of financial information. *See* 16 C.F.R. § 314. These requirements could turn out to be inconsistent with any regulations adopted in the instant proceeding.

Congress is also considering bills that would strengthen the tools available to target pretexters themselves. Indeed, there are numerous bills pending before Congress dealing with data security and the sale of telephone records.<sup>3</sup> There are also indications that Congress may

---

<sup>3</sup> For example, H.R. 4662 prohibits obtaining telephone records through “false pretenses” and requires that a carrier notify a customer when the customer’s records are disclosed to someone other than the customer; H.R. 4378 prohibits obtaining or selling phone records by false pretenses; H.R. 4709 prohibits obtaining phone records through fraud; the sale of such records or the purchase of such records if the buyer knows they were obtained without authorization; S. 2178 is the companion bill to H.R. 4709. *See* Gina Marie Stevens and Tara Alexandra Rainson, *Data Security: Protecting the Privacy of Phone Records*, CRS Report at 8 (Feb. 28, 2006) (“*CRS Report*”).

mandate data retention, at least with respect to ISPs.<sup>4</sup> Any or all of these bills could obviate the need for any federal agency regulations. It is clear, therefore, that the prudent course for the FCC now is to hold off on serious consideration of any regulations until Congress has made its final decision as to how best to address pretexting.

*Second*, if and when adopted, federal agency regulations should be narrowly tailored to address the problem of pretexting and should not impose unnecessarily onerous requirements on parties solely because they happen to fall within a particular agency's jurisdiction. In practice, this means that the FCC should not adopt pretexting regulations targeted at carriers and indeed may not be the appropriate agency to address pretexting more generally. Carriers, the only entities clearly within the FCC's jurisdiction in this context, already have powerful incentives to protect the confidentiality of CPNI, and carriers are in any event already subject to adequate legal requirements that they do so. Adding to those requirements would increase carriers' compliance costs and reduce their ability to serve their customers without materially diminishing pretexting. Carriers' incentive to protect CPNI is derived from straightforward business realities. A carrier's customers' CPNI is a critical asset that enables a carrier to identify, for example, opportunities for selling new services to existing customers.

In addition, a carrier would suffer severe reputational harm if it were to fail to protect its customers' CPNI. Nearly all of TWTC's customers are either medium to large size enterprises or carriers that demand the highest level of security and are particularly sensitive about any loss

---

<sup>4</sup> See Declan McCullagh, *ISP Snooping Gaining Support*, CNETNEWS.COM (Apr. 14, 2006), available at [http://news.com.com/ISP+snooping+gaining+support/2100-1028\\_3-6061187.html](http://news.com.com/ISP+snooping+gaining+support/2100-1028_3-6061187.html) ("At a hearing last week, Rep. Ed Whitfield, a Kentucky Republican who heads a House oversight and investigations subcommittee, suggested that data retention laws would be useful to police investigating crimes against children.").

of their confidential information. If the confidentiality of a customer's CPNI were compromised or if TWTC were revealed to have lax security, TWTC's business would suffer.

This was exactly ChoicePoint's experience. After ChoicePoint disclosed that it lacked adequate protections for its customers' data, the company's stock price dropped sharply.<sup>5</sup> ChoicePoint's Chief Information Security Officer observed at the time that the perception that ChoicePoint does not safeguard its customer's information is "killing ChoicePoint[s] [reputation] . . . . That's such a negative impression that suggests we failed to provide adequate protection."<sup>6</sup> It seems likely that any carrier in a similar situation would experience similar harm.

In addition to their powerful business incentive to protect the confidentiality of CPNI, carriers are of course subject to statutory prohibitions that act as a backstop against the unlikely situation in which a carrier would want to share or disclose CPNI inappropriately. Sections 222(a) and (c) establish unambiguous requirements that carriers "protect the confidentiality of proprietary information of, and relating to . . . customers" (47 U.S.C. § 222(a)) and "use, disclose, or permit access to individually identifiable customer proprietary network information"

---

<sup>5</sup> Indeed, ChoicePoint shareholders initiated a shareholder derivative suit against ChoicePoint for the loss in the stock's value following the disclosure that ChoicePoint was not adequately protecting their customers' information. See Joris Evers, *Shareholders Sue ChoicePoint: The Company's Share Price Has Dropped More Than 20% In A Month*, COMPUTERWORLD (Mar. 7, 2005), available at <http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,100239,00.html> ("Shareholders are suing ChoicePoint Inc. and its top executives after the company's share price fell sharply following news that identity thieves had gained access to personal information about some U.S. residents that was held by the personal data vendor.") (emphasis added).

<sup>6</sup> Mike Mimoso, *ChoicePoint CISO on the hot seat but also firing back*, SEARCHSECURITY.COM, (Feb. 24, 2005), available at [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1062076,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1062076,00.html).

in only narrowly defined circumstances (*id.* § 222(c)). Carriers obviously have the incentive to comply with these requirements even if they for some reason lack the normal powerful incentive to protect the confidentiality of their customers' CPNI. For all of these reasons, it is not surprising that carriers generally have implemented robust processes and procedures for protecting the confidentiality of CPNI.<sup>7</sup>

Moreover, the fact that bad actors have fraudulently obtained CPNI from carriers does not mean that further regulation of *carriers* would be either effective or efficient. Pretexting has occurred notwithstanding carriers' strong desire to prevent it.<sup>8</sup> It is hard to see how the government could do a better job in this regard than that companies themselves. Indeed, none of the proposals for carrier regulation discussed in the NPRM would likely materially reduce instances of pretexting. At the same time, all of those proposals would, if adopted, increase carrier costs, in some cases substantially.

To begin with, the proposals set forth in the *EPIC Petition* are uniformly flawed. For example, any technical standards, such as the mandatory password and encryption standards proposed by EPIC, could only be effective if all parties that receive CPNI from a carrier secure their systems adequately. Carriers in many cases transmit CPNI to third parties to perform

---

<sup>7</sup> See *CRS Report* at 1 (noting that “[p]hone companies are believed to have strict rules preventing and guarding against the employee sale of telephone records and the unauthorized acquisition of customer information”).

<sup>8</sup> It is a reflection of carriers' wholesome incentives in the area of CPNI that carriers themselves have initiated private suits against pretexters, underscoring their incentive and commitment to protect their customers' information. See, e.g., *Cingular Wireless LLC v. Data Find Solutions, Inc.*, *James Kester, 1st Source Information Specialists, Inc.*, *Kenneth W. Gorman, Steven Schwartz, John Does 1-100, and XYZ Corps. 1-100*, No. 05-3269, Compl. ¶ 21 (D.N.D. Ga. filed Dec. 23, 2005).

critical functions such as telemarketing, installation and repair.<sup>9</sup> Because the Commission does not have jurisdiction over non-carriers in this context, it could only enforce mandatory password or encryption standards against carriers. Thus, carriers might alone be responsible for ensuring that all parties comply with new detailed password or encryption regulations. Carriers would then be presented with the Hobson's Choice of either foregoing sharing CPNI with most or all third parties that perform legitimate and important business functions or policing the practices of separate companies that might not have the technical ability or resources to implement the FCC's detailed regulations.

Even if EPIC's proposed technical rules were necessary (and they are not), the FCC should not be in the business of designing rigid technical standards. The FCC has largely avoided mandating specific technical standards in the past for the sensible reason that, as a slow-moving government agency, it cannot keep abreast of the latest and most appropriate technologies. To the extent that the FCC does impose technical requirements, they are usually *functional* and the FCC generally does not mandate a particular standard or technology.

In fact, in a departure from its normal practice, the FCC adopted in a 1998 order extremely detailed rules for how the database containing the customer's CPNI election should be

---

<sup>9</sup> Carriers currently have an obligation to enter into a "confidentiality agreement" with any third party independent contractor or joint venture partner that may receive CPNI to ensure that adequate safeguards are in place to prevent disclosure of that information. *Implementation of the Telecommunications Act of 1996 et al.*, Third Report and Order, 17 FCC Rcd 14860, ¶ 47 (2002) ("In particular, we require carriers, at a minimum, to enter into confidentiality agreements with independent contractors or joint venture partners that . . . require that the independent contractor or joint venture partner have appropriate protections in place to ensure the ongoing confidentiality of consumers' CPNI."). When it adopted these regulations, however, the Commission sensibly did not establish detailed requirements regarding how this obligation must be satisfied.

maintained (the so-called “flagging requirement”).<sup>10</sup> On reconsideration, the FCC eliminated the detailed flagging requirement and permitted carriers to monitor their customers’ CPNI elections in a manner that was appropriate for each individual carrier. It did so to “allow the carriers the flexibility to adapt their record keeping systems in a manner most conducive to their individual size, capital resources, culture and technological capabilities.”<sup>11</sup> The same considerations should prevent the adoption of one size fits all technical requirements in the instant situation.

The Commission has declined to fashion detailed technical guidelines of its own on many other occasions. Most recently, even in the face of a clear public policy crisis caused by the failure of some VoIP providers to provide adequate 911 service, the Commission directed that interconnected VoIP providers provide E911 capability, but did not dictate how that functionality should be provided.<sup>12</sup> When it has imposed detailed requirements, they are usually designed by an “expert” organization and then ratified by the Commission (something that does not exist in the present context). For example, in its local number portability (“LNP”) orders and rules the FCC mandated only functional requirements.<sup>13</sup> Many LNP technical standards, to the extent that

---

<sup>10</sup> See, e.g., *Implementation of the Telecommunications Act of 1996*, Second Report and Order, 13 FCC Rcd 8061, ¶ 198 (1998) (“We specifically require that carriers develop and implement software systems that ‘flag’ customer service records in connection with CPNI. Carriers have indicated that their systems could be modified relatively easily to accommodate such CPNI ‘flags.’ The flag must be conspicuously displayed within a box or comment field within the first few lines of the first computer screen.”).

<sup>11</sup> See *Implementation of the Telecommunications Act of 1996*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, ¶ 7 (1999) (“*CPNI Reconsideration Order*”).

<sup>12</sup> See generally *IP Enabled Services et al.*, First Report and Order, 20 FCC Rcd 10245 (2005).

<sup>13</sup> See, e.g., 47 C.F.R. § 52.31(a) (“[A]ll covered CMRS providers must provide a long-term database method for number portability.”). The FCC did not mandate a particular database design or detailed technical requirements.

they were mandated, were developed by NANC and later ratified by the FCC.<sup>14</sup> NANC has the expertise to develop technical porting standards in ways that the Commission does not.

Similarly, the FCC did not mandate the technical standards for “Plug-and-Play” cable systems, but rather left the development of the standard to negotiations between the content industry and device manufacturers, the parties with the requisite expertise.<sup>15</sup>

As InfoNXX notes in its comments on the *EPIC Petition*,<sup>16</sup> any technical standards set by the FCC would not be flexible enough to respond to the changing tactics and methods of pretexters. It is highly unlikely that the FCC could anticipate every move made and method employed by these bad actors. On the other hand, carriers, that have the incentive to protect their customers’ data, as well and the technical knowledge and business experience to do so effectively, should be allowed the discretion necessary to protect their customers’ data in the manner that they believe will be most effective.

In addition to these shortcomings, each of EPIC’s specific proposals suffers from substantial problems that counsel against adoption. Many the arguments against EPIC’s

---

<sup>14</sup> See, e.g., *Telephone Number Portability et al.*, Memorandum Opinion and Order, 18 FCC Rcd 23697, ¶ 7 (2003) (“In 1997, in the Local Number Portability *Second Report and Order*, the Commission adopted recommendations from the North American Numbering Council (NANC) for the implementation of wireline-to-wireline number portability. Under the guidelines developed by the NANC, porting between LECs was limited to carriers with facilities or numbering resources in the same rate center to accommodate technical limitations associated with the proper rating of wireline calls.”).

<sup>15</sup> See *Implementation of Section 304 of the Telecommunications Act of 1996*, Second Report and Order, 18 FCC Rcd 20885, ¶ 7 (2003) (noting that industry negotiations have completed with respect to the technical specification for unidirectional devices but are ongoing with respect to bi-directional devices).

<sup>16</sup> See Comments of InfoNXX, Inc., CC Dkt. No. 96,115 *et al.*, at 6 (filed Apr. 14, 2006).

proposals have already been raised by commenters in response to EPIC's petition for rulemaking.

*Customer Passwords.* As Verizon and Verizon Wireless argued, transaction of legitimate business would be hampered by a customer password requirement.<sup>17</sup> Those parties argued that customers often do not contact carriers for months at a time, and may have forgotten the password by the time they need to speak with a carrier. *See Verizon Comments* at 3. As a result, carriers that offer online access to customers via password protected accounts receive a large number of requests for password assistance.<sup>18</sup> Since carriers must provide some method for consumers to reset forgotten passwords, wrongdoers will eventually adapt their techniques to take advantage of those procedures. *See Verizon Comments* at 4. To reset a password, all that a pretexter would typically need is a phone number, an address and other personal or confidential data that a pretexter has already obtained through illicit means before he or she has even contacted the carrier to obtain the customer's CPNI.<sup>19</sup> Moreover as CTIA has explained,<sup>20</sup> and Cingular argued in its recent suit against pretexters (*see supra* note 8), pretexters can often obtain the password itself through fraudulent means.

---

<sup>17</sup> *See* Comments of Verizon, Dkt. No. 96-115 *et al.*, at 3-4 (filed Oct. 31, 2005) ("*Verizon Comments*"); Comments of Verizon Wireless, Dkt. No. 96-115 *et al.*, at 6-7 (filed Oct. 31, 2005) ("*Verizon Wireless Comments*").

<sup>18</sup> *See* CTIA - The Wireless Association Comments in Opposition to EPIC Petition for Rulemaking, Dkt. No. 96-115 *et al.*, at 18 (filed Oct. 31, 2005) ("*CTIA Comments*").

<sup>19</sup> *See EPIC Petition* at 8 (noting that pretexters can easily obtain dates of birth, mothers' maiden names, or social security numbers).

<sup>20</sup> *See* Testimony of Steve Largent, President and CEO of CTIA-The Wireless Association, Before the House of Representatives Committee on Energy and Commerce at 3 (Feb. 1, 2006) (attached to Letter of Paul Garnett, CTIA, to Marlene H. Dortch, Secretary, FCC, CC Dkt. No. 96-115 *et al.* (Feb. 2, 2006)).

The Commission asks whether the use of a “shared secret” would improve the utility of passwords. *CPNI NPRM* ¶¶ 15-16. At least with respect to carriers such as TWTC serving large businesses, the answer is clearly no. Typically, many employees in the large companies served by TWTC must be able to access the company’s account. Under a password/shared secret system, all employees who must access a company’s account would also require access to (and be required to remember) the password and shared secret. It is likely that many situations would arise in which an employee either does not know or has forgotten the password or the shared secret. In such situations, the password and/or the shared secret would need to be reset using information already in the possession of the pretexter.

*Audit Trails.* There is no reason to think, and EPIC has offered none, that audit trails would limit pretexting. Carriers usually do not know when a customer record has been improperly accessed via pretexting, thus making it impossible even to know when to initiate an audit trail. Even assuming the carrier or customer were to subsequently determine when the customer’s CPNI had been accessed through fraud, all that the audit trail would indicate is that the “customer” called on x date at y time asking for its CPNI. This information is obviously completely unhelpful to identifying the pretexter or preventing pretexting in the future.

Moreover, audit trails would be extremely costly to implement. The FCC previously mandated, and then subsequently eliminated an audit requirement. In eliminating the requirement, the FCC determined that the cost of compliance could reach \$270 million for each carrier, while the incremental increase in security would have been minimal.<sup>21</sup> The FCC therefore sensibly concluded that the costs of audits outweighed the benefits: “[a]s it is already

---

<sup>21</sup> See Opposition of BellSouth Corporation, Dkt. No. 96-115 *et al.*, at 5 (filed Oct. 31, 2005) (“*BellSouth Comments*”) (citing *CPNI Reconsideration Order* ¶ 123).

incumbent upon all carriers to ensure that CPNI is not misused and that our rules regarding the use of CPNI are not violated, we conclude, on balance, such a potentially costly and burdensome rule does not justify its benefit.” *CPNI Reconsideration Order* ¶ 127. There is no reason to believe that this calculus has changed in the 6 years since the FCC eliminated this requirement. For example, in its comments regarding the *EPIC Petition*, BellSouth reasoned that, if the cost in the 1990s reached \$270 million, today those figures would be significantly greater. *See BellSouth Comments* at 5. Although the burdens on a company the size of BellSouth would undoubtedly be high, the financial burden would be even greater for smaller carriers such as TWTC, that would be required to spread the cost of similar systems upgrades over a much smaller revenue base. Indeed, it is most unlikely that small competitive carriers, such as TWTC, would ever be able to recover such costs from its customers. Even at half the cost previously estimated by the FCC, imposition of this requirement on small carriers would threaten their ability to remain viable businesses.

*Notification Requirements.* A requirement that carriers notify their customers in the event of a security breach is also unlikely to address the problem of pretexting. As mentioned, carriers do not generally know when pretexters have obtained access to customer records. They cannot therefore notify their customers that pretexting has occurred, regardless of their duty to do so. Other proposed notification requirements, such as calling the customer’s registered telephone number before releasing CPNI (*see CPNI NPRM* ¶ 22), are unworkable. For example, if a company employee in New York is legitimately requesting CPNI, but the carrier will only release CPNI if it can reach an employee at the company’s registered number in Los Angeles, substantial delay and confusion will likely result.

*Encryption Requirements.* Even putting aside the standards-related issues discussed above, EPIC's proposed encryption requirement suffers for fundamental flaws. While encryption might be useful to prevent hacking, that is not a problem implicated by pretexting. Indeed, there is no evidence indicating that "hacking" of carriers' systems is occurring. CTIA and Verizon have also correctly explained that the cost of developing encryption systems would be unreasonably large. Verizon estimated that development and implementation of encryption systems could cost the industry hundreds of millions of dollars. *See CTIA Comments* at 19; *Verizon Comments* at 4-5. Just as high costs and uncertain results led the FCC to eliminate its audit trail and flagging requirements, these same factors counsel against the imposition of an encryption requirement, especially for smaller carriers such as TWTC. Indeed, the FCC did not require that carriers establish electronic systems to monitor customers' CPNI elections in the past, because many carriers could not afford such systems and the cost and disruption of implementation far outweighed the incremental gain in security. *See CPNI Reconsideration Order* ¶ 125. If some carriers could not afford electronic record keeping in 1999, there is no reason to believe that these same carriers could bear the cost of both digitizing their records and implementing an encryption requirement today.

*Limiting Data Retention of Call Details.* Limiting access to call detail information would probably limit the ability of pretexters to obtain CPNI, but it would come at an unreasonably high price. Such an approach is akin to giving away half of your jewelry so that it will not fall into the hands of a robber. Call detail information is used for a myriad of legitimate customer service purposes and its elimination or limiting its availability would harm consumer welfare. As CTIA explained, CPNI records are used for, among other things, assisting customers who need to validate charges on their bills, assisting customers who need to document past events for

the sake of resolving potential billing problems and cooperating with law enforcement in criminal and national security matters. *See CTIA Comments* at 19.

Indeed, law enforcement's use of stored customer information is absolutely crucial to solving crimes. The Attorney General only last week castigated ISPs for not retaining user logs for a long enough period for the FBI to adequately conduct sex crimes investigations.<sup>22</sup> The retention of phone records is equally important in assisting the prosecution of crimes. Recognizing the importance of retaining customer data, the EU has recently enacted tough data retention policies for phone and internet providers to help fight terrorism and organized crime.<sup>23</sup> Under the law, ISPs and carriers must keep customer records for up to two years. *See id.* The need to access customer records to deter crime and terrorism is no less urgent in the U.S. than the EU.

Finally, in addition to the proposals discussed in the *EPIC Petition*, the Commission requested comment on whether it should mandate opt-in approval for CPNI disclosures to third party independent contractors and joint venture partners. *See CPNI NRPM* ¶ 12. A move to an opt-in regime would be both bad policy and constitutionally impermissible. As noted previously, carriers must, in the normal course of business, provide CPNI to contractors, such as sales and marketing partners, on a regular basis. In TWTC's experience, it is extremely difficult for carriers to obtain opt-in consent. Therefore, if opt-in were mandated, numerous carrier operations that rely on independent contractors would likely grind to a halt. Indeed, TWTC did

---

<sup>22</sup> Anne Broache, *U.S. Attorney General Calls for 'Reasonable' Data Retention*, CNETNEWS.COM (Apr. 20, 2006), available at [http://news.com.com/U.S.+attorney+general+calls+for+reasonable+data+retention/2100-1030\\_3-6063185.html](http://news.com.com/U.S.+attorney+general+calls+for+reasonable+data+retention/2100-1030_3-6063185.html).

<sup>23</sup> Jo Best, *EU Data Retention Directive Gets Final Nod*, CNETNEWS.COM (Feb. 22, 2006), available at [http://news.com.com/EU+data+retention+directive+gets+final+nod/2100-7348\\_3-6042032.html](http://news.com.com/EU+data+retention+directive+gets+final+nod/2100-7348_3-6042032.html).

not even attempt to use CPNI for marketing campaigns during the period when only opt-in approval was permitted for use of CPNI; it would have been too difficult to obtain the requisite permissions. It is TWTC's belief that the failure to obtain approval is largely the result of customer inertia, not a particular fear that customers may have regarding the disclosure of their CPNI. Nor does the manner of the customer's CPNI election have anything to do with the problem of pretexting. There have been no indications that customer data has been compromised or somehow made more easily available to bad actors in those situations where the Commission currently permits carriers to use opt-out notices and elections.

Furthermore, the Tenth Circuit struck down the Commission's mandatory use of opt-in on First Amendment grounds, and there is no reason to think that the court would come to a different conclusion if opt-in were again mandated.<sup>24</sup> The court analyzed the opt-in rule under the three part analysis established in *Central Hudson*.<sup>25</sup> Under that analysis, as long as the commercial speech is not misleading, the government may restrict the speech only if 1) it has a substantial state interest in regulating the speech; 2) the regulation directly and materially advances that interest; and 3) the regulation is no more extensive than necessary ("narrowly tailored") to serve that interest. *See US West*, 182 F.3d at 1233. The Tenth Circuit found that the commercial marketing activities affected by the CPNI rules were "commercial speech" and that the privacy interest which the government sought to advance in its opt-in rules (preventing embarrassing personal disclosures) was "substantial," thereby satisfying the first prong. *Id.* at 1236. However, the court determined that the opt-in regime failed the second and third prongs,

---

<sup>24</sup> *U.S. W., Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999) ("*US West*").

<sup>25</sup> *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557 (U.S. 1980) ("*Central Hudson*").

because the regulation did not materially advance this interest and, even if it did, the opt-in rules were not narrowly tailored. *Id.* at 1237-39.

Chairman Martin has recently acknowledged the hard limits that this ruling places on the FCC. In recent testimony to Congress, Chairman Martin asked Congress to “overturn the ruling of a federal court that limited the Commission’s ability to implement more stringent protection of consumer phone information.”<sup>26</sup> Absent such an outcome the Commission cannot ignore the constraints identified in the *US West* case.

The discussion above in fact demonstrates that regulations targeted at carriers are inherently ill-suited to addressing pretexting. But this does not mean that no remedies exist. Rather than imposing ineffective and costly regulation on carriers, federal and state governments should focus on prosecuting pretexters themselves under existing laws. Indeed, states and the FTC have all taken action against pretexters under current statutes and enforcement activity is picking up steam. Pretexters are relatively easy to identify because they have electronic storefronts on the internet that must be easily accessible for customers to purchase information. Their relative accessibility has made them an easy target for enforcement and legal action.

For example, in 2001, the FTC launched “operation pretext” against businesses that were pretexting for personal financial information, and filed three lawsuits,<sup>27</sup> all of which were

---

<sup>26</sup> See Testimony of Kevin Martin, Before the House of Representatives Committee on Energy and Commerce at 9 (Feb. 1, 2006).

<sup>27</sup> *FTC v. Victor L. Guzzetta, d/b/a/ Smart Data Systems*, No. 01-2335 (E.D.N.Y.) (final judgment entered Feb. 25, 2002); *FTC v. Information Search, Inc., and David Kacala*, No. 01-1121 (D. Md.) (final judgment entered Mar. 15, 2002); *FTC v. Paula L. Garrett, d/b/a Discreet Data Systems*, No. 01-1255 (S.D. Tex.) (final judgment entered Mar. 25, 2002).

settled.<sup>28</sup> Not only were these companies accused of violating the Graham-Leach-Bliley Act (“GLBA”), which only applies to financial records, but also Section 5 of the FTC Act which bans “unfair and deceptive” practices. The FTC’s Section 5 authority is broad. The FTC has stated that it may use Section 5 to pursue pretexters who are attempting to obtain phone records: “Although pretexting for consumer telephone records is not prohibited by the GLBA, the Commission may bring a law enforcement action against a pretexter of telephone records for deceptive or unfair practices under Section 5 of the FTC Act.” *Liebowitz Testimony* at 7. Indeed, the FTC (apparently in response to EPIC’s complaint) is currently investigating pretexters who attempt to obtain telephone records and “Commission attorneys currently are evaluating the evidence to determine if law enforcement action is warranted.” *Id.* at 8.

Numerous states, including Florida,<sup>29</sup> Illinois,<sup>30</sup> Missouri,<sup>31</sup> and Texas<sup>32</sup> have all sued data

---

<sup>28</sup> See Prepared Statement of Jon Liebowitz, Commissioner of the FTC Before the Committee on Energy and Commerce, U.S. House of Representatives at 4-5 (Feb 1, 2006) (“*Liebowitz Testimony*”) (“In each of these cases, defendants advertised that they could obtain non-public, confidential financial information, including information on checking and savings account numbers and balances, stock, bond and mutual fund accounts, and safe deposit box locations . . . . The FTC alleged that the defendants or persons they hired called banks, posing as customers, to obtain balances on checking accounts.”). All agreed to settlements with the FTC. *See id.* at 15.

<sup>29</sup> See *Florida v. 1<sup>ST</sup> Source Information Specialists, Inc.*, No. 37-2006-CA-000234, Compl. for Injunctive and Other Statutory Relief (Leon County filed Jan. 24, 2006) (“*Florida AG suit*”).

<sup>30</sup> Press Release, *Office of the Attorney General, Madigan Sues Second Company that Sells Cell Phone Records* (Mar. 15, 2006), available at [www.ag.state.il.us/pressroom/2006\\_03/20060315c.html](http://www.ag.state.il.us/pressroom/2006_03/20060315c.html) (“Attorney General Lisa Madigan [on Mar. 15, 2006] filed a lawsuit against a Florida company that allegedly obtained and sold the phone records of individuals without their knowledge or consent.”) (“*Illinois AG Announcement*”).

<sup>31</sup> Press Release, Missouri Attorney General’s Office, *Locatecell.com must stop selling cell phone records of Missourians, under court order obtained by Nixon* (Feb. 15, 2006), available at [www.ago.mo.gov/newsreleases/2006/021506.htm](http://www.ago.mo.gov/newsreleases/2006/021506.htm) (“Attorney general Jay Nixon on Tuesday (Feb. 14) obtained court orders to stop the sale of Missourians’ cell phone records by several

brokers for pretexting phone records. Both Connecticut and Massachusetts have begun investigations of pretexters' operations. *See CRS Report* at 9. Many of these states are suing under their existing "little FTC acts" which prohibit unfair and deceptive practices.<sup>33</sup> Nearly every state has a similar law, making enforcement against phone pretexters a real possibility in nearly every state. This is precisely the type of government initiative that is efficiently targeted at pretexting and that should obviate FCC action.

*Third*, even if the FCC were to adopt pretexting regulations, it should not apply them mechanically to all carriers. The agency should instead consider a carrier's customer base and a carrier's size when determining whether to apply such regulation to a particular class of carriers. For example, there is no basis for applying such new regulations to carriers serving enterprise

---

(continued)

people currently or formerly associated with the Web site Locatecell.com. On Jan. 20, Nixon sued the defendants for violating state consumer protection laws.”).

<sup>32</sup> Press Release, Attorney General of Texas, *Attorney General Abbott Files First Suit Against Sellers Of Private Phone Records* (Feb. 9, 2006), available at <http://www.oag.state.tx.us/oagnews/release.php?id=1449> (“Texas Attorney General Greg Abbott today filed the state’s first lawsuit against a ‘data broker’ and his companies – USA Skiptrace, AMS Research Services Inc. and Worldwide Investigations Inc. – for fraudulently marketing consumers’ private phone records.”).

<sup>33</sup> *See Florida AG Suit* ¶¶ 1, 13 (“This is an action for temporary and permanent injunctive relief, brought pursuant to the Florida Deceptive and Unfair Trade Practices Act . . . . Plaintiff brings this action to stop Defendants from unlawfully obtaining and disseminating confidential customer telephone records and information through fraud and deception, to stop Defendants from selling such records and information over the internet, and to stop the Defendants from advertising on their websites that they will sell such records to members of the public.”); *Illinois AG Announcement* (“Madigan’s complaint seeks to prohibit the defendants from operating in Illinois and seeks civil penalties [for violations of] the Illinois Consumer Fraud and Deceptive Business Practices Act.”); *Texas v. John Strange, d/b/a/ USA Skiptrace.com*, No. 06-1666, Compl. ¶ 9.2 (Travis County) (“Defendants, as alleged and detailed above, have in the course of trade and commerce engaged in false, misleading and deceptive acts and practices declared unlawful in §§ 17.46(a) and (b) of the [Texas Deceptive Trade Practices and Consumer Protection Act]”).

customers. Neither EPIC nor any other party has proffered any meaningful evidence that pretexting is a problem facing business customers or carriers, like TWTC, that exclusively serve business customers. Nearly all of the evidence in the record indicates that that pretexters are attempting to obtain calling data from consumers in order to snoop on cheating spouses or provide information to stalkers or to people who want to cause other individuals harm. For instance, in response to an EPIC complaint, one data broker listed the myriad uses for its services. All of those services were focused on tracking or locating individuals.<sup>34</sup> No commenter has provided a convincing explanation as to why a pretexter would want to obtain the CPNI of a business or that pretexting of business customers actually occurs. The only relevant mention by EPIC is a conclusory claim of “industrial espionage” without any support.<sup>35</sup> Moreover, even if pretexting were a problem in the business market, as discussed above, many of the safeguards proposed by EPIC would be particularly ill-suited for that market.

Similarly, the Commission should avoid imposing regulations that require significant fixed compliance costs on smaller carriers. As explained above, there are several proposals such as those for audit trails and encryption that would impose proportionately a far greater burden on smaller than larger carriers. The Commission must consider these in determining whether to impose such requirements on smaller carriers. In the case of smaller carriers that serve only enterprise customers, it should be clear that the costs far outweigh any conceivable benefits.

---

<sup>34</sup> See Letter from EPIC to FTC, at 4 (Aug. 30, 2005) (attached to *EPIC Petition*) (“Law enforcement, private investigators, attorneys and many industry experts contend that cell phone and landline based call records help parents locate missing and runaway children; help solve crimes; bail bondsman locate fugitives; insurance companies refute fraudulent claims; collection agencies track down deadbeats; financial institutions locate people and collocators; and yes, spouses find out if their significant other is being faithful or cheating.”).

<sup>35</sup> See *EPIC Petition* at 9 (noting that pretexting “*could be* (and most likely are being) used for industrial espionage . . .”) (emphasis added).

