FEDERAL COMMUNICATIONS COMMISSION

CC DOCKET NO. 96-115

AND

WC DOCKET NO. 04-36

Further Notice of Proposed Rulemaking: Customer Proprietary Network Information

COMMENTS OF:

CONSUMER ACTION
CONSUMER FEDERATION OF AMERICA
CONSUMERS UNION
ELECTRONIC PRIVACY INFORMATION CENTER
NATIONAL CONSUMERS LEAGUE
PRIVACY ACTIVISM
PRIVACY JOURNAL
PRIVACY RIGHTS CLEARINGHOUSE
U.S. PUBLIC INTEREST RESEARCH GROUPS
UTILITY CONSUMERS' ACTION NETWORK

July 9, 2007

TABLE OF CONTENTS

I. Introduction 1
II. Background 2
III. Carriers Must Verify Customer Identity Prior to Disclosure of Account Information 6
IV. Audit Trails Aid Prosecution of Pretexters 8
V. Internal Physical Safeguards Strengthen Protection of CPNI 9
A. Encrypt All CPNI 10
B. Minimize Carrier Employee Access to CPNI 10
C. Implement Audit Trails to Track Carrier Employee Access 12
VI. Limiting Data Retention Reduces Customer Vulnerability 12
VII. Personal Information on Cell Phones Creates Privacy Risks 14
A. Simplify Procedures for Customer-Side Deletion of Cell Phone Data 15
B. Carriers Must Erase Cell Phone Data Prior to Recycling 16
C. Carriers Must Implement Remote Deletion for Lost or Stolen Phones 17
D. Manufacturers Should Implement a Hardware Solution for Data Deletion 19
VIII. Additional Recommendations to Protect Customer Privacy 20
A. Carriers Must Immediately Notify Customers of Data Breaches 20
B. Establish a Comprehensive Opt-In Policy 22
1. Current Opt-out Policy Provides Inadequate Coverage & Notice 22
2. Opt-out Policy Inflates Consumer Transaction Costs 23
3. Carriers Must Notify Customers of Data Recipients 24
C. Consumer Coalition Commends the Commission for Extending CPNI Protections to VoIP 25
IX. Conclusion 26

I. Introduction

By notice published on June 8, 2007, the Federal Communications Commission ("FCC" or "Commission") announced a Notice of Proposed Rulemaking ("NPRM") seeking comments on further privacy protections for Customer Proprietary Network Information ("CPNI").[1] Pursuant to this notice, the aforementioned groups ("Consumer Coalition") submit these Comments to request the FCC to promulgate further safeguards protecting customers' telephone records.

The Consumer Coalition believes the sale of CPNI could result in serious and irreversible privacy problems for customers. To the extent that the Commission allows any sale of CPNI, we maintain that such sale should be allowed only if the recipient is a telecommunications provider with whom the customer has a current business relationship, and an opt-in mechanism is provided to customers. To protect against abuses of customer information, the Consumer Coalition recommends that the Commission enact rules that require carriers to (1) expand password protection, (2) maintain audit trails, (3) encrypt all CPNI, (4) limit employee access to CPNI, (5) limit data retention, (6) safeguard information stored in cell phones, and (7) curtail law enforcement-related delay of customer notification of security breaches. We also urge the Commission to (8) adopt a comprehensive opt-in policy. Finally, we commend the Commission for expanding its rules to include protections for VoIP services.

These recommendations carry substantial benefits to carriers both large and small. Moreover, strong privacy safeguards reduce the number of security breaches, thereby reducing the financial costs associated with repairing the breach and reducing the extent of harm done to carriers' reputations when a breach occurs. A 2007 Forrester Research survey estimated that

[1] Fed. Commc'ns Comm'n, *Notice of Proposed Rulemaking: Customer Proprietary Network Information*, 72 Fed. Reg. 110, 31782 (June 8, 2007) [hereinafter "NPRM"], *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/E7-10734.htm.

security breaches cost $90 to $305 per lost record.[2] A 2007 McAfee study found that a breach that exposed personal information would cost companies an average of $268,000 just to inform their customers, and a third of respondents believed a major breach would put them out of business altogether.[3] These costs might be especially hard on small carriers with more limited resources.

Most importantly, these safeguards defend consumer privacy at a time when data security tops the list of consumer concerns. In 2006, the Federal Trade Commission listed identity theft as the No. 1 consumer complaint for the seventh year in a row, accounting for 36 percent of filed complaints and generating more than five times the amount of complaints of the second-place item.[4] Finally, strong privacy safeguards enhance customers' trust and goodwill in their carriers.

II. Background

On August 30, 2005, EPIC petitioned the Federal Communications Commission to initiate rulemaking to enhance security safeguards for individuals' calling records. In its Petition EPIC noted that through Section 222 of the Telecommunications Act of 1996,[5] Congress has "specifically placed the burden of protecting Customer Proprietary Network Information (CPNI) in [telecommunications carriers] hands."[6] CPNI is the data collected by telecommunications corporations about a consumer's telephone calls. It includes the time, date, duration and destination number of each call, the type of network a customer subscribes to, and any other

[2] Sharon Gaudin, *Security Breaches Cost $90 to $305 Per Lost Record*, INFORMATION WEEK, Apr. 11, 2007, *available at* http://www.informationweek.com/news/showArticle.jhtml?articleID=199000222.
[3] McAfee, *Datagate: The Next Inevitable Corporate Disaster?* 3, 9, Apr. 24, 2007, *available at* http://www.softcat.com/files/pdfs/McAfee_Datagate_White_paper.pdf.
[4] Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.
[5] 47 U.S.C. § 222 et seq. (2006).
[6] EPIC, In the matter of Implementation of the Telecommunications Act of 1996, Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, CC Docket No. 96-115, before the Fed. Commc'ns Comm'n (Aug. 30, 2005) [hereinafter "EPIC Petition"].

information that appears on the customer's telephone bill.[7] EPIC's Petition called for the FCC to immediately initiate a rulemaking proceeding to address CPNI protection measures used by carriers, and to invite comment to develop adequate safeguards for verifying the identity of parties trying to access CPNI.[8] EPIC suggested five forms of security measures that could be used by carriers to more adequately protect access to CPNI: customer-set passwords, security breach notification, audit trails, encryption, and limiting data retention.[9]

The telecommunications industry quickly responded to EPIC's Petition, urging the FCC to take enforcement actions against companies that sell phone records, but opposing any regulatory intervention that would require carriers to change their security standards.[10] EPIC responded, pointing out that enforcement actions against online data brokers alone are unlikely to prevent the sale of phone records, and that "FCC intervention is necessary to enhance security standards and authentication standards for access to CPNI."[11] Carriers responded that no additional rules were necessary, and urged the FCC to deny EPIC's Petition.[12]

In January 2006, after news reports[13] regarding the vulnerability of phone records to online data brokers surfaced, Sen. Harry Reid sent a letter to the FCC, urging the agency to "begin an investigation into how online data brokers are obtaining Americans' private phone records, and whether phone companies are doing enough to protect the personal and private

---

[7] 47 U.S.C. § 222 et seq. (2006).
[8] EPIC Petition, *supra* note 6.
[9] *Id.*
[10] *See, e.g.*, Opposition of BellSouth Corporation to EPIC Petition, RM Docket No. 11277 (Oct. 31, 2005).
[11] EPIC, Reply Comments In the matter of Implementation of the Telecommunications Act of 1996, Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, CC Docket No. 96-115, before the Fed. Commc'ns Comm'n (Nov. 9, 2005), *available at* http://epic.org/privacy/iei/epicfccreply.pdf.
[12] *See* CTIA – The Wireless Association, Reply Comments to EPIC Reply Comments In the Matter of Electronic Privacy Information Center, Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, CC Docket No. 96-115, RM Docket No. 11277, before the Fed. Commc'ns Comm'n (Nov. 15, 2005), *available at* http://www.epic.org/privacy/iei/ctiareply.pdf.
[13] *See, e.g.*, John Reinan, *Illegal sales of call records are raising government and industry alarm*, STAR TRIBUNE (Minn., MN), Jan. 22, 2006, at A1.

information with which they are entrusted."[14] On January 17, 2006, FCC Commissioners Jonathan Adelstein and Michael Copps released statements calling for action to address the illegal sale of telephone records.[15] Commissioner Adelstein noted that EPIC's Petition "could be an appropriate vehicle for tightening [the FCC's] rules."[16]

On February 10, 2006, the FCC approved EPIC's Petition, seeking comment on the five measures EPIC suggested to improve security of CPNI, as well as other measures.[17] The comment deadline was April 14, 2006. A coalition of consumer and civil liberties groups joined EPIC in filing comments with the FCC.[18] The comments focused on the failure of phone carriers to shield customer information from private investigators and online data brokers who use pretexting. In particular, the coalition argued that the use of biographical identifiers as passwords, such as the Social Security number and date of birth, has made phone records vulnerable to pretexting. These identifiers are widely available to pretexters through subscriptions to commercial data broker services.

On June 8, 2007, the FCC published new rules in the Federal Register on April 2, 2007.[19] The Final Order, which strengthens the privacy protections of CPNI, is the Commission's response to the practice of pretexting.[20] The new rules require customers to provide a password

---

[14] Letter from Harry Reid, U.S. Senator, to Kevin Martin, Chairman, Fed. Commc'ns Comm'n (Jan. 13, 2006), *available at* http://www.epic.org/privacy/iei/reidltr1.13.06.pdf.

[15] Press Release, Fed. Commc'ns Comm'n, Statement by Commissioner Jonathan S. Adelstein on Brokering of Personal Telephone Records (Jan. 17, 2006) [hereinafter "Commissioner Adelstein's Statement"], *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263216A1.doc; Press Release, Fed. Commc'ns Comm'n, Commissioner Michael J. Copps Calls for Action to Address Theft of Phone Records (Jan. 17, 2006) [hereinafter " Commissioner Copps's Statement"], *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A3.pdf.

[16] Commissioner Adelstein's Statement, *supra* note 15.

[17] *See* 21 F.C.C.R. 1782, 1789 (2006).

[18] Reply Comments of the Electronic Privacy Information Center, CC Docket No. 96-115, RM Docket No. 11277 (Apr. 14, 2005).

[19] Fed. Commc'ns Comm'n, *Final Rule: Customer Proprietary Network Information*, 72 Fed. Reg. 110, 31948 (June 8, 2007) (to be codified at 47 C.F.R. pt. 64) [hereinafter "Final Rule"], *available at* http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/E7-10732.htm.

[20] *Id.* at 31,949.

when customers call a carrier before the carrier can release customers' phone call records.[21] The new rules also require the customer to receive notice of any changes made to their account information.[22] The rules also include a requirement that carriers notify customers of unauthorized disclosures of telephone records; however, law enforcement agencies can delay notification.[23] Commissioners Adelstein and Copps both criticized this provision.[24]

Previous regulations prohibited disclosure of call detail information to third parties offering non-communications-related services without the express, or opt-in, consent of customers. The FCC's new rules extend the requirement of opt-in consent to joint venture partners and independent contractors.[25] In addition, the rules require carriers to file with the Commission an annual certification, including an explanation of any actions taken against data brokers and a summary of all consumer complaints received in the previous year regarding the unauthorized release of CPNI.[26] The Final Order also extends all CPNI rules to cover providers of interconnected voice over Internet Protocol ("VoIP") service.[27]

The Final Order imposes a general duty on carriers to take "every reasonable precaution" to prevent unauthorized disclosure of CPNI, and it creates a presumption of a violation of that duty in any case of unauthorized disclosure of information.[28] Since the FCC has previously established that carriers are directly responsible for the actions of their agents in safeguarding CPNI, this duty means that carriers now need to take particular care to ensure that any contracts

---

[21] *Id.*
[22] *Id.*
[23] *Id.* at 31,950.
[24] *See* Statement of Commissioner Michael J. Copps, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services,* Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 96-115 and WC Docket No. 04-36 (Apr. 2, 2007) [hereinafter "Statement of Copps on CPNI"]; Statement of Commissioner Jonathan S. Adelstein [on same topic] (Apr. 2, 2007) [hereinafter "Statement of Adelstein on CPNI"].
[25] Final Rule, *supra* note 19, at 31,950.
[26] Press Release, Fed. Commc'ns Comm'n, FCC Strengthens Privacy Rules To Prevent Pretexting (Apr. 2, 2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-272008A1.pdf.
[27] *Id.*
[28] Final Rule, *supra* note 19, at 31,951.

with third parties upon whom they rely in providing their services include obligations to comply with the limitations set forth in the FCC's newly revised CPNI rules.[29]

In its Petition, EPIC proposed five security measures, listed above, that would more adequately protect access to call detail information.[30] The FCC addressed the first two security measures in its rule, and announced an NPRM to consider expanded password protection, audit trails, encryption, data retention, and safeguards for information stored in cell phones.[31] Comments are due July 9, 2007, and reply comments are due on or before August 7, 2007.[32]

In response to the NPRM, the Consumer Coalition respectfully submits the following Comments.

III. Carriers Must Verify Customer Identity Prior to Disclosure of Account Information

The Commission requests comments on the following:

Should the FCC extend these rules to include optional or mandatory password protection for non-call detail CPNI? Should this password protection be for all non-call detail CPNI or should it only include certain account changes? If the FCC were to adopt password protection for certain account changes, what should that include (e.g. changes in the address of record, account plans, or billing methods)?[33]

The Consumer Coalition commends the Commission for requiring password protection for customer-initiated telephone contact that results in the divulging of call-detail information. In addition, the Commission has also required the provision of a password for online access, photo identification for in-person help, and notification to customers after certain account changes.[34]

---

[29] E-mail Alerts, Wilmer Hale, FCC Releases New Rules for Safeguarding Customer Proprietary Network Information in Response to Pretexting (Apr. 9, 2007), *available at* http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=3648.
[30] *See* EPIC Petition, *supra* note 6.
[31] *See* NPRM, *supra* note 1, at 31,782.
[32] *Id.*
[33] *Id.* at 31,783.
[34] These account changes include whenever a password, customer response to a carrier designed back-up means of authentication, online account, or address of record is created or changed. Final Rule, *supra* note 19, at 31,949.

However, the Commission should require a customer's identity to be verified by a mandatory password before the release of any information, call detail or non-call detail CPNI, related to that customer's account. Password protection ensures that the proper individual accesses the proper account. Thus, to allow an individual the opportunity to bypass one of the two identity safeguards (password and name) only opens a loophole for pretexters to exploit, thereby defeating the purpose of the new rules.

Simply providing mere notice to customers of account changes or attempts to access information to an account, absent any password requirement, does not offer adequate protection. Most customers do not understand the term CPNI, and even if this term is defined most customers will not connect CPNI with its privacy implications.[35] Consequently, the protection of customer CPNI must start with the carriers. Those carriers must implement a mandatory password protocol connected to the release of any customer information.

Finally, a broad rule requiring a password to access any form of customer or account information removes confusion among customers as to when or whether one must provide a password. Carriers can easily implement this rule, as it would require minimal staff training. Such a rule also simplifies the burden for carriers in determining whether a carrier's employees followed standard operating procedure with customer identity verification. It would also be helpful if the Commission considered how to assist consumers with simple requests that may not necessitate a password or the release of sensitive data.

[35] For example, Verizon's CPNI notice does not contain the word "privacy" (although it does appear on the privacy policy Web site) nor does it explicitly state the fact that CPNI includes a person's calling records. *See* Verizon, Privacy and Customer Security Policies – Telephone Company Customer Policy, http://www22.verizon.com/about/privacy/customer/; Sprint's CPNI notice fully defines CPNI, but follows the definition with an explanation that a customer's name, address, and telephone number are not CPNI. While true, this confuses customers as to whether the disclosure of CPNI to third parties is truly harmful. *See* Sprint, Sprint Privacy Policy, http://www.sprint.com/legal/sprint_privacy.html; T-Mobile buries its definition of CPNI under its "full privacy policy" which must be accessed from its "privacy highlights" page, *see* T-Mobile, T-Mobile Privacy Policy, http://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_PrivacyNotice&print=true#fullpolicy.

IV. Audit Trails Aid Prosecution of Pretexters

The Commission requests comments on the following:

Are audit trails generally used by carriers to track customer contact? Would an audit trail assist law enforcement in criminal investigations against pretexters? Have carriers' reactions to audit trails changed or has the technology changed such that the audit trails are now an economically feasible option?[36]

The Consumer Coalition renews its call for auditing of those who access CPNI. While the FCC astutely notes that the vast majority of inquiries into a customer's phone records are legitimate,[37] numbers alone should not dictate a policy choice. Rather, record access should be audited to prevent improper disclosure of personal information maintained by communications companies.

Firms often employ suspect data brokers in order to obtain phone records. In 2006, congressional investigators subpoenaed the records of suspect data brokers. The customers of these brokers included the finance units of Honda, Ford, DaimlerChrysler, Citigroup, J.P. Morgan Chase, and Wells Fargo & Co. The same investigators also found examples of law enforcement employing firms suspected of pretexting, in order to acquire phone numbers.[38]

Moreover, the art of pretexting encompasses more than simply data brokers. Pretexting played a central role in a case involving Hewlett-Packard and suspected leaks by its insiders to the media. In order to determine which insiders leaked information, Hewlett-Packard hired private investigators that utilized pretexting to acquire the personal phone records of board members and journalists in an effort to locate the source of the leaks.[39] Even before the Hewlett-

[36] NPRM, *supra* note 1, at 31,783.
[37] *See id.*
[38] *See* John R. Emshwiller, *Old Trick: Hewlett-Packard Was Far From First To Try 'Pretexting'*, WALL. ST. J., Dec. 16, 2006, at A1.
[39] Charges against the former chairwoman were eventually dismissed. *See* Matt Richtel, *Charges Dismissed in Hewlett-Packard Spying Case*, N.Y. TIMES, Mar. 15, 2007, at C1.

Packard case, in 2005, the *Wall Street Journal* reported on bank employees who sold the information of 500,000 account holders:

> Experts say the breach could have been avoided if the banks had detected abnormal activities on their computer systems early on. The employees involved would normally have accessed 30 to 40 customer records in a normal business day, according to police. As the theft occurred the employees were sometimes accessing 300 to 400 customer records a day - an anomaly that could have been spotted had the right protections been in place.[40]

Further, the use of an audit trail to show a repeated pattern of pretexting over multiple accounts can prove invaluable in prosecuting offenders to the fullest extent of the law, thereby deterring others from engaging in similar practices. Finally, carriers routinely track customer service inquiries for their own internal purposes.[41] As a result, most carriers own the infrastructure required to record all attempts to access a customer's record, reducing the burden on implementing this system.

V. Internal Physical Safeguards Strengthen Protection of CPNI

The Commission requests comments on the following:

Whether it should adopt rules that govern physical transfer of CPNI among companies, such as between a carrier and its affiliates, or the transfer of CPNI to any other third party authorized to access or maintain CPNI, including a carrier's joint venture partners and independent contractors. What physical safeguards are carriers currently using when they transfer or allow access to CPNI to ensure that they maintain the security and confidentiality of CPNI? Are these safeguards sufficient? What steps should the Commission require of a carrier to protect CPNI when CPNI is being transferred or accessed by the carrier, its affiliates, or its third parties? What are the benefits and burdens, including the burdens on small carriers, of requiring carriers to physically safeguard the security and confidentiality of CPNI?[42]

---

[40] Li Yuan, *Companies Face System Attacks From Inside, Too*, WALL ST. J., Jun. 1, 2005, at B1.

[41] *See* Verizon, Privacy and Consumer Security Policies – Telephone Company Customer Privacy, http://www22.verizon.com/about/privacy/customer/ ("Verizon obtains information about customers that helps us to provide service, and we use that information for business purposes only . . . When you call us, a service representative refers to your customer record to serve you better.") (cited for proposition that carriers track customer service inquiries); AT&T, AT&T Privacy Policy, http://www.att.com/gen/privacy-policy?pid=2506 ("We use the personal identifying information of a customer to provide, confirm, change, bill, monitor and resolve problems with the quality of AT&T-offered products and services.") (cited for proposition that carriers track customer service inquires).

[42] *See* NPRM, *supra* note 1, at 31,783.

A. Encrypt All CPNI

The Consumer Coalition requests the FCC to require carriers to encrypt stored CPNI. Encryption safeguards the confidentiality of the data from unauthorized employees inside the carrier, and also protects against security breach from data thieves outside the carrier. While encryption of stored CPNI may be costly, sensitive customer information, collected without the affirmative consent of the consumer, should not be exposed to increased vulnerability simply because encryption does not appeal to a carrier's cost-benefit analysis.[43]

For example, the Federal Trade Commission recommends that businesses consider encrypting sensitive information stored on networks, disks, laptops and other portable storage devices used by employees.[44] Moreover, a number of major carriers already employ encryption protocols for transmission of information and when customers view their data online.[45] Broadening such protocols to cover stored CPNI is a reasonable extension of carriers' preexisting practices. Perhaps most importantly, the cost of storing and encrypting CPNI could most easily be reduced if overall carriers retained a lesser amount of CPNI. Carriers can best accomplish this by adopting an opt-in regime with regard to the use of CPNI for marketing purposes. An opt-in policy would make great strides towards protecting customer privacy and reducing the volume of unwanted service solicitations.

B. Minimize Carrier Employee Access to CPNI

The more information is shared, the greater the risk that data may be acquired by dishonest

[43] Qwest, Comments before the FCC on Implementation of the Telecommunications Act of 1996 10, Apr. 28, 2006, CC Docket No. 96-115 [hereinafter "Qwest Comments"].
[44] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Businesses* 10, 14, http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf.
[45] *See* Sprint, Sprint Privacy Policy, Network and Information Security, http://www.sprint.com/legal/sprint_privacy.html#network; AT&T, AT&T Privacy Notice, How We Protect Your Information, http://www.att.com/gen/privacy-policy?pid=7666#108; Qwest, Qwest Online Privacy Policy, What does Qwest do to help safeguard personal information collected online?, http://www.qwest.com/privacy; Verizon, Verizon Internet Privacy Policy, How does Verizon protect my personal information?, http://www22.verizon.com/privacy.

employees or others who have access to data in the course of its transfer. There is increasing evidence that insiders who have access to personal data present serious risks for identity theft and other fraud.

The 2006 Chief Security Officer E-Crime Watch survey of corporate security executives and law enforcement reported that insiders committed 56 percent of thefts of customer records and proprietary information, and that employees committed 46 percent of identity thefts against their employer's own customers.[46] A 2004 study conducted by the Federal Deposit Insurance Corporation reported that "industry analysts and security professionals estimate that 65 to 70 percent of identity theft is committed with confidential information stolen by employees or participants."[47] A 2004 news report covering a study from Michigan State University indicated that a researcher found in a review of 1,000 identity theft cases that between 50 to 70 percent were insider jobs.[48]

In light of this threat, carriers should be instructed to minimize the number of insiders in contact with CPNI. The Federal Trade Commission recommends that businesses restrict CPNI access to employees with a legitimate business need.[49] Carriers can accomplish this in many ways, such by establishing different electronic permission levels for employees based on their job function.[50] Some major carriers already indicate that they follow such a policy.[51] The

---

[46] Press Release, CSO Magazine, Survey Shows E-Crime Incidents Are Declining Yet Impact Is Increasing: 2006 E-Crime Watch Survey from CSO Mazine Reveals Insider Threats Are On The Rise (Sept. 6, 2006), *available at* http://www2.csoonline.com/info/release.html?CID=24531.

[47] Fed. Deposit Ins. Corp., *Putting an End to Account-Hijacking Identity Theft* 10, Dec. 14, 2004, *available at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[48] Bob Sullivan, *Study: ID theft usually an inside job; Up to 70 percent of cases start with employee heist*, MSNBC, May 21, 2004, *available at* http://www.msnbc.msn.com/id/5015565/.

[49] FTC, Protecting Personal Information: A Guide for Businesses, http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf, at 10.

[50] Microsoft, Limit Employee Computer Access, *available at* http://www.microsoft.com/australia/smallbusiness/themes/winxp/article3.mspx.

[51] *See* Sprint Privacy Policy, Network and Information Security, http://www.sprint.com/legal/sprint_privacy.html#network; AT&T Privacy Notice, How We Protect Your

Consumer Coalition now requests the Commission to require carriers to limit the number of their employees with access to CPNI and other personal information only to those who must do so to carry out their duties. Audit trails can further protect against insider abuse.

C. Implement Audit Trails to Track Carrier Employee Access

The Consumer Coalition requests that the FCC require carriers to establish audit trails to track carrier employee contact with CPNI. Audit trails deter insiders from selling personal information, and once data is accessed without authorization, audit trails aid in investigating the security breach. Carriers should be under a duty to record all instances where a customer's record is accessed, who accessed the information, and for what purpose. This can be accomplished, for example, by requiring employees to log instances in which they access servers or physically transport drives containing CPNI.

Some major carriers have similar systems in place to prosecute unauthorized employee access.[52] Requiring carriers to maintain such a system by law would further protect against unauthorized release of confidential information and offer more assistance in tracking those responsible. Minimizing the number of carrier employees with access to personal information can reduce audit trails. Utilizing a comprehensive opt-in CPNI policy would reduce the quantity of audit trails, reducing the costs that carriers must incur to protect customer privacy.

VI. Limiting Data Retention Reduces Customer Vulnerability

The Commission requests comments on the following:

Whether it should adopt rules that require carriers to limit data retention. Does a limitation on data retention enhance protection of CPNI? What should be the maximum amount of time that a carrier should be able to retain customer records? Additionally, should all customer records be eliminated or is there a subset of customer records that are more susceptible to abuse and should be destroyed? Should the Commission define exceptions where a

---

Information, http://www.att.com/gen/privacy-policy?pid=7666#108; Verizon General Privacy Principles, Information Management and Security, *available at* http://www22.verizon.com/about/privacy/genpriv/#7.

[52] Qwest Comments, *supra* note 43, at 13.

carrier is permitted to retain certain records? Alternatively, should the Commission require *carriers to de-identify customer records after a certain period? The FCC seeks comment on the benefits and burdens, including the burdens on small carriers, of requiring carriers to limit their data retention or to de-identify customer records.*[53]

A limitation on data retention enhances protection of CPNI. Retention limitations reduce the severity of security breaches by shrinking the quantity of aggregated data vulnerable to those who would misuse it from both within and without the carrier. Such reductions are necessary because of the almost-daily occurrence of security breaches of sensitive personal information. Over 158 million data records of U.S. residents have been exposed due to security breaches since January 2005, according to a report from the Privacy Rights Clearinghouse.[54]

The Consumer Coalition urges the Commission to require CPNI records to be deleted immediately after they are no longer needed for billing or dispute purposes. While some major carriers currently state in their privacy principles that individual customer information is retained for business purposes only, the scope of "business purposes" is expansive.[55] AT&T, for example, provides CPNI to its agents and affiliates to market products, services, packages, and promotions to its customers, whether those customers are interested or not.[56] Such a business purpose may extend for many years, for as long as the customer maintains an account. During this time, the CPNI is stored with the carrier under limited encryption and audit trail security standards.

Moreover, personally identifiable information, such as Social Security numbers, account numbers, billing information and contact lists are targets for identity thieves and should be eliminated as soon as the information is no longer needed for billing or a dispute. Likewise, calling history, the location of the caller, and calendar and speed dial data are vulnerable to

[53] *See* NPRM, *supra* note 1, at 31,783.
[54] Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[55] *See* Verizon Telephone Company Customer Privacy, The Information We Obtain and How We Use It, http://www22.verizon.com/about/privacy/customer/; Sprint Privacy Policy, Retention of Information, http://www.sprint.com/legal/sprint_privacy.html#retention.
[56] AT&T Privacy Notice, Use of CPNI, http://www.att.com/gen/privacy-policy?pid=2566.

misuse by stalkers, harassers and domestic abusers and should be eliminated as soon as such data is no longer needed for billing or a dispute. Time and duration of calls may be less vulnerable and would still enable carriers to suggest some service-related offers to its customers.

Deletion is the most secure and certain way to eliminate risk. If de-identification is selected as a viable option, such a protocol should require carriers to divorce identification data from transactional records. This would allow carriers to maintain call records for data analysis but reduce, though not eliminate, the risk that the same records could later be associated with an account holder. De-identification may not eliminate the possibility that the data can be re-identified through data recovery or drive reconstitution.

Although forbidding sale of CPNI based on aggregated data amounts to a lost source of revenue, carriers would enjoy the enhanced customer trust and goodwill resulting from strong privacy protection. Restricting retention decreases carrier costs associated with data storage, as well as the financial burdens resulting from security breaches. Most importantly, limiting data retention protects customer privacy and reduces the severity of data breach when such breach occurs.

VII. Personal Information on Cell Phones Creates Privacy Risks

The Commission requests comments on the following:

What steps should the FCC take, if any, to secure the privacy of customer information stored in mobile communications devices?[57]

The Consumer Coalition requests the FCC promulgate rules that secure the privacy of customer information stored in mobile communications devices. At the end of 2006, there were 233 million wireless subscribers in the United States, with more than 76 percent of the total

[57] NPRM, *supra* note 1 at 31,784.

population owning a cell phone.[58] During the month of December 2006, Americans sent 18.7 billion text messages.[59] Vast amounts of information are stored on cell phones, including e-mail on smart-phones. According to a survey sponsored by software maker Symantec Corp., 37 percent of smart-phone users store confidential business data on their phones.[60] Only 40 percent of those surveyed worked at companies that have corporate policies about wireless security.[61]

Software can be cheaply purchased that allows purchasers of refurbished or used cell phones to retrieve personal information from them, even if the previous owner thought he or she had deleted all of the information.[62] When phone are refurbished, lost or stolen, consumers' personal information is compromised unless they are given the ability to permanently delete that information. While some carriers offer data deletion services, there is no uniform policy. The FCC should act now to protect personal data on cell phones.

A. Simplify Procedures for Customer-Side Deletion of Cell Phone Data

Currently, no uniform federal rule requires manufacturers or carriers to provide customers with easy ways to permanently delete information stored on cell phones. A test conducted by Trust Digital, a mobile security software company, highlights the problem. The company recovered 27,000 pages of personal, corporate, and device data from nine of 10 mobile devices purchased through eBay.[63] The salvaged data included personal banking and tax information, corporate sales activity notes, corporate client records, product roadmaps, contact

[58] CTIA – The Wireless Association, Wireless Quick Facts, Dec. 2006, http://www.ctia.org/advocacy/research/index.cfm/AID/10323.
[59] *Id.*
[60] Yuki Noguchi, *Lost a Blackberry? Data Could Open a Security Breach*, July 25, 2005, WASH. POST at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/07/24/AR2005072401135.html.
[61] *Id.*
[62] Ted Bridis, *Secrets linger on old cell phones*, HOUSTON CHRONICLE, Aug. 31, 2006, at A1.
[63] Press Release, Trust Digital, Used Smartphones and PDAs for Sale on eBay Reveal Massive Volume of Sensitive Data (Aug. 30, 2006), *available at* http://www.trustdigital.com/news/press/2006_0830.asp.

address books, phone and Web logs, calendar records, personal and business correspondence, computer passwords, user medication data and other potentially damaging information.[64]

A popular practice among sellers of recycled phones, that of "resetting" a phone, often means sensitive information appears to have been erased, but it can be resurrected using specialized yet inexpensive software found on the Internet.[65] Because consumers upgrade their cell phones on average about every 18 months,[66] there are a number of people utilizing recycling programs. It takes flash memory longer to erase information in ways that make it impossible to recover, so manufacturers compensate with methods that erase the data less completely but do not make a phone seem sluggish.[67]

Computer disk drives operate in a similar way, allowing identity thieves to find traces of personal information on discarded computers with hard drives that have not been completely erased. A number of companies provide software that will permanently erase hard drives.[68] In addition to computers, most Internet browsers now have a feature that allows customers to delete the record of items that a customer has seen, heard, or downloaded from the Web, often referred to as "cache" data.[69]

The Consumer Coalition requests that the FCC require carriers and manufacturers to configure wireless devices so consumers can easily and permanently delete personal information from those devices. The FCC should also require carriers to permanently erase all information on cell phones before refurbishing and reselling them.

B. Carriers Must Erase Cell Phone Data Prior to Recycling

---

[64] *Id.*
[65] Bridis, *supra* note 61.
[66] *Id.*
[67] *Id.*
[68] *See, e.g.*, Secure Delete, http://www.secure-delete.net.
[69] Microsoft, How and Why to Clear Your Cache, http://www.microsoft.com/windows/ie/ie6/using/howto/customizing/clearcache.mspx.

The Commission requests comments on the following:

What methods are carriers currently using, if any, for erasing customer information on mobile equipment prior to refurbishing the equipment, and to what extent do carriers enable customers to permanently erase their personal information prior to discarding the device? Should the FCC require carriers to permanently erase, or allow customers to permanently erase, customer information in such circumstances?[70]

Of the major wireless carriers offering recycling programs, Verizon Wireless is the only carrier that says explicitly on its Web site that a vendor scrubs the phone of all personal data as part of the refurbishing process before distributing it for reuse.[71] Verizon,[72] Sprint,[73] T-Mobile[74] and AT&T[75] all encourage customers utilizing their recycling program to clear data off their phone before they recycle it. T-Mobile's site reads, "Please make sure to delete all personal information stored on the phone. We are not responsible for any consequences related to failure to delete personal information."[76]

The FCC should require carriers to permanently erase personal data before refurbishing and reselling a cell phone. Carriers should inform the customer that sensitive personal information could still reside on a phone before that customer is allowed to recycle it. Carriers should give customers the option of permanently erasing their phones before turning them in to be recycled.

C. Carriers Must Implement Remote Deletion for Lost or Stolen Phones

A separate problem is presented to customers whose cell phones are lost or stolen. In these instances, some carriers provide for remote data deletion. For example, Sprint can delete

[70] NPRM, *supra* note 1, at 31,784.
[71] Verizon, Verizon Wireless HopeLine Answers to FAQs, http://support.vzw.com/faqs/Company%20Information/faq_hopeline.html.
[72] *Id.*
[73] Sprint, Sprint Project Connect FAQs, http://www.sprint.com/community/communities_across/project_connect.html.
[74] T-Mobile Handset Recycling, http://www.t-mobile.com/Company/Community.aspx?tp=Abt_Tab_HandsetRecycling.
[75] AT&T Reuse & Recycle, http://www.wireless.att.com/about/community-support/recycling.jsp.
[76] T-Mobile Handset Recycling, *supra* note 73.

information by sending a signal to a phone over the air, although if the device is turned off, the "kill" signal won't work.[77] A *Washington Post* article explains the problem in better detail:

> Companies are peeling back some of the convenience of mobile devices in favor of extra layers of password protection and other restrictions. Some are installing software on their networks to make it impossible to download corporate information to a portable device or a memory stick, which is a plug-in device that holds data for use on other computers.
>
> Security companies have come up with ways to install layers of password protection and automatic locks on devices. Others market the ability to erase data over the air once the device is reported lost. In Japan, cell phone carrier NTT DoCoMo Inc. started selling models that come with fingerprint scanners to biometrically unlock phones.[78]

The FCC should require carriers to provide a service, similar to Sprint's kill service, which would delete personal information remotely in the case of a lost or stolen cell phone. This service should be provided only if a customer can properly identify himself or herself and provide a password. The FCC should also require carriers to include in the software installed on mobile phone devices an easy way for customers to permanently delete personal information.

The amount of personal data that exists on customers' phones could translate into huge security breaches in the event that the phone is lost or stolen. To protect consumer privacy, the FCC should require carriers to give options to the consumer for preventing or minimizing the effects of such thefts. Although the costs of implementing the above suggestions might be substantial and might affect small carriers disproportionately, the Consumer Coalition believes instituting a uniform, industry-wide data deletion policy is necessary to protect CPNI. While it may be more expensive to obtain the technology for remote data deletion, it would be relatively cheap for carriers to incorporate a permanent delete feature into the software installed on their phones.

---

[77] Noguchi, *supra* note 59.
[78] *Id.*

D. Manufacturers Should Implement a Hardware Solution for Data Deletion

The Commission requests comment on the following:

Should the Commission require manufacturers to configure wireless devices so consumers can easily and permanently delete personal information from those devices?[79]

The FCC should require manufacturers to configure cell phones so consumers can easily and permanently delete personal information. The FCC could require that manufacturers make data deletion easier, perhaps by making it an option on the phone's menu or by creating a single "reset" button that permanently deletes the information on the phone. This could be patterned after reset buttons on watches and other devices. The FCC should also require manufacturers to display data deletion information prominently in the phones' manuals.

Phone manufacturers usually provide obscure or inconvenient instructions for deleting a customer's information. For example, Palm, Inc., which makes the Treo smart-phone, puts directions deep within its Web site for what it calls a "zero out reset."[80] It involves holding down three buttons simultaneously while pressing a fourth tiny button on the back of the phone. A number of other phones have similarly complicated methods for completely erasing information.

Though there is a risk that consumers might press the reset button by accident and permanently lose their personal information, manufacturers could reduce that risk by patterning the reset button after those on many wireless routers, which require a sharp object to activate. Other options include putting the reset button behind the battery so it is only accessible by taking the battery out of the phone or requiring that the reset button be held down for several seconds.

The FCC should require manufacturers to make flash memory cards easily removable like SIM cards. Cell phones offered by T-Mobile and AT&T currently have SIM cards that store

[79] NPRM, *supra* note 1, at 31,784.
[80] Bridis, *supra* note 61.

a cell phone's number and up to 250 contacts.[81] The advantage of a SIM card is that it can be easily removed from a cell phone and transferred to a new phone. However, cell phones still use flash memory to store applications and code. If this is done, when a consumer recycles a phone, he or she can take out the flash card and the SIM card. At that point, no personal information about the consumer would remain on the phone. While this requirement might come at a substantial cost to manufacturers, the Consumer Coalition believe it is necessary for the entire industry to start addressing privacy concerns.

VIII. Additional Recommendations to Protect Customer Privacy

A. Carriers Must Immediately Notify Customers of Data Breaches

In addition to the comments above, the Consumer Coalition also agrees with the statements of Commissioners Copps and Adelstein on the law enforcement notification scheme in the event of a breach.[82] The current scheme allows law enforcement to refrain from notifying an individual of a breach for up to 14 days. Such a period may be extended "as long as reasonably necessary in the judgment of the agency."[83] As Commissioner Adelstein noted, "Under these rules, the Commission gives the Federal Bureau of Investigation a potentially open-ended ability to delay customer notification of security breaches . . . automatic delays coupled with unlimited extensions are not appropriate."[84]

We would like to remind the Commission that it is not merely data brokers who engage in pretexting.[85] Rather, private investigators, jilted lovers, and those seeking to stalk or harass other individuals also pretext, and it is the individual harms caused by these persons that most

[81] CNET, *SIM Card Explained*, Apr. 12, 2005, http://reviews.cnet.com/4520-10166_7-6160666-1.html.
[82] *See* Statement of Copps on CPNI, Statement of Adelstein on CPNI, *supra* note 24.
[83] Final Rule, *supra* note 19, 31,963. Law enforcement refers to the Federal Bureau of Investigation and the Secret Service. *Id.*
[84] Statement of Adelstein on CPNI, *supra* note 24.
[85] *See supra* Part III for examples of pretexting in the corporate context.

implicates the need for immediate disclosure to the affected customer. In addition, many perpetrators seek information for clients involved in divorces or other civil disputes.[86]

Notification allows customers the chance to minimize or prevent any harms resulting from this breach. In particular, victims of spousal abuse are in the best position to recognize the violator, know the harm heading their way, and with adequate notification, can best aid law enforcement in deterring this harm. For example, a police officer in Wisconsin unlawfully disclosed a victim's address to a stalker. The stalker immediately sent the victim a note, resuming a pattern of harassment.[87] The speed with which the stalker reacted to this information leak demonstrates the perils already facing a domestic violence victim. To allow law enforcement to wait up to 14 days in the case of a CPNI-related data breach would only exacerbate this danger. Consequently, all customers must be notified as soon as possible in the event of a security breach.

However, occasional exigent circumstances might arise where immediate notification could compromise national security. In the rare event of such a circumstance, a delay in notification may be sanctioned. This delay must be limited to no more than seven (7) days, and should require formal notification to the agency head.[88] In addition, such circumstances must truly be exigent, and the harm of disclosure "immediate and irreparable,"[89] as customers have a right to protect their own data and act upon notification of a breach.

---

[86] *See* Matt Richtel, *With Just a Little Stealth, Anyone Can Get Phone Records,* N.Y. TIMES, Sept. 7, 2006, at C9. Cell phone records are equally vulnerable to pretexters. *See* Matt Richtel, *House Panel to Press Cellphone Industry on Improving Protection of Customer Records*, N.Y. TIMES, Feb. 1, 2006, at C3. In 2006, a blogger purchased the cell phone records of General Wesley Clark for $89.95. Congress has since moved to criminalize the access of consumer phone records through pretexting, but criminal penalties do not correct the inherent lack of security in the system. *See* Frank Ahrens, *When a Stranger Calls, Beware of The Pretext*, WASH. POST, Sept. 9, 2006, at D1.
[87] Kevin Murphy, *Officer's Actions will Cost 25,000*, GAZETTEXTRA, Feb. 15, 2007, *available at* http://www.gazetteextra.com/mezera021507.asp (last visited June 19, 2007).
[88] *See* EPIC, Comments of the Electronic Privacy Information Center to the Federal Trade Commission, Apr. 3, 2007 (regarding Identity Theft Task Force) for the inspiration behind this rule.
[89] Final Rule, *supra* note 19, at 31,951.

B. Establish a Comprehensive Opt-In Policy

The Consumer Coalition would like to reiterate that a comprehensive opt-in approach is the only truly effective means to provide privacy protection to those consumers who desire it. As Commissioner Michael Copps stated, "[a] customer's private information should never be shared by a carrier with any entity for marketing purposes without a customer opting-in to the use of his or her personal information."[90] Likewise, carriers must provide customers with clear and conspicuous notice of their right to opt-in. On behalf of tens of millions of telephone customers in the United States, we respectfully urge the Commission to limit the sale or transfer of sensitive customer information, and condition any sale or transfer of CPNI on both the provision of proper notice to affected subscribers, and on an opt-in approval mechanism.

1. Current Opt-out Policy Provides Inadequate Coverage & Notice

The Consumer Coalition commends the Commission for taking the step to require carriers to obtain customer consent prior to providing personal information to joint venture partners and independent contractors. However, we continue to urge the FCC to require a comprehensive opt-in approach towards telecommunications carriers' use of CPNI pursuant to Section 222 of the Telecommunications Act of 1996. Absent affirmative denial of consent from the customer, the Commission currently permits a carrier to use its customers' individually identifiable CPNI for marketing purposes, and also to disclose and provide access to CPNI to the carrier's agents and affiliates that offer such marketing services.[91]

This opt-out approach is inadequate because it is not calculated to reasonably inform consumers about their privacy options, and often customers may not know that they must affirmatively act to prevent carrier distribution of their CPNI. Under opt-out approaches,

[90] Statement of Copps on CPNI, *supra* at 24.
[91] NPRM, *supra* note 1, at 31,962.

customers bear the burden of paying for and returning their opt-out notice. Such notices are often written in complex language that customers have neither patience nor ability to read, and are often concealed amongst less important "junk mail" notices from the same source.[92]

2. Opt-out Policy Inflates Consumer Transaction Costs

Proponents of an opt-out approach may argue that such a system is economically preferable, as it increases the amount of information available to both producers and consumers, allows telecommunications carriers to tailor their services to specific customers and reduces prices.[93] Yet this assertion erroneously assumes that the only costs at issue are those of production, without accounting for increased transaction costs incurred by the consumers seeking to exercise privacy rights created by statute.[94] Opt-out regimes create an economic incentive for businesses to make it difficult for consumers to exercise their preference not to disclose personal information to others.[95] Because opt-out systems do not require businesses to create inducements for consumers to choose affirmatively to disclose personal information, these systems encourage firms to engage in strategic behavior and thus inflate consumer transaction costs.[96]

In contrast, an opt-in system would permit consumers who wish to protect their privacy to do so, while encouraging telecommunications carriers to eliminate consumer transaction costs.[97] Because carriers profit from the use of consumer information, and thus want as much information as possible, carriers would have an incentive to make it as easy as possible for

---

[92] Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices* (July 2001), *available at* http://www.privacyrights.org/ar/GLB-Reading.htm.
[93] *See* AT&T Corp., Comments In the Matter of Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, CC Docket No. 96-115, CC Docket No. 96-149 at i, Nov. 01, 2001.
[94] *See* Jeff Sovern, *Toward A New Model of Consumer Protection: The Problem of Inflated Transaction Costs,* 47 WM & MARY L. REV. 1635, 1644 (2006).
[95] *Id.*
[96] *See* Jeff Sovern, *Opting in, Opting Out, or No Options at All,: The Fight For Control of Personal Information,* 74 WASH. L. REV. 1033, 1099-1100 (1999).
[97] *Id.*

consumers to consent to the use of their personal information. Such a system might include a comprehensible list of the benefits to opting-in, contained within a clearly marked mailing, with a pre-paid stamped envelope. This would preclude the transaction costs involved with attempting to contact via phone customers with the authority to opt-in. It also reduces the strategic behavior costs associated with opt-out — the costs associated with providing consumers a message that they do not want consumers to receive — because the carriers would have an incentive to lower costs associated with providing customers a message that they are very eager to have the customer receive.[98] Finally, opt-in might decrease the amount of information in the marketplace, but it permits carriers to target products at those who have specified an interest in such information, thereby decreasing the wasted costs associated with targeting uninterested customers.[99]

3. Expressly Notify Customers of Data Recipients

Although an opt-in policy is highly preferable, a possible alternative may be for the Commission to require carriers to inform each customer of the identity of every affiliate, agent or entity to whom the customer's personal information and CPNI has been disclosed for marketing purposes. This notice could be included with monthly billing statements, should be written clearly and conspicuously, and should alert the customer to any change in the list of companies who have received his or her information. Such a system would be quite similar to that established under California law.[100] While we support customers' right to full disclosure regarding data collection and use, notice alone is less protective than a blanket opt-in policy that would safeguard everyone, including those who cannot or do not read notices.

---

[98] *Id.* at 1101-02.
[99] *Id.* at 1103.
[100] *See* Calif. Civ. Code §1798.83; Calif. Pub. Util. Code §2891(b).

C. Consumer Coalition Commends the Commission for Extending CPNI Protections to VoIP

In the Order, the FCC explained that while it has not decided whether interconnected VoIP services are "telecommunications services" or "information services" under the Communications Act, the Commission's Title I ancillary jurisdiction allows it to impose the CPNI rules on interconnected VoIP providers.[101] In the wake of recent similar developments pertaining to the Communications Assistance for Law Enforcement Act (CALEA), universal service, and 911 requirements, VoIP providers are likely to see the application of the CPNI rules as yet another move in the wrong direction — imposing "legacy" telecom rules on this new generation of voice service.[102]

In a letter written to the FCC, the VON Coalition, a group of VoIP providers, argued that CPNI rules should not be extended to VoIP providers because of the differences between traditional telecommunications and interconnected VoIP.[103] The VON Coalition argues, among other reasons, that applying CPNI requirements to them is unnecessary because they are already subject to federal and state privacy restrictions.[104] The VON Coalition also points out that VoIP could be a part of the solution:

> As EPIC pointed out in testimony before Congress – as more people switch to VoIP, pretexting problems may simply "disappear" 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 appear to require – could actually

[101] Final Rule, *supra* note 19, at 31,950.
[102] E-mail Alerts, Wilmer Hale, FCC Releases New Rules for Safeguarding Customer Proprietary Network Information in Response to Pretexting (Apr. 9, 2007), *available at* http://www.wilmerhale.com/publications/whPubsDetail.aspx?publication=3648.
[103] *See* Letter from VON Coalition to Marlene Dortch, Sec'y, Fed. Trade Comm'n (Jan. 31, 2007) [hereinafter "VON Letter"], *available at* http://www.von.org/usr_files/Privacy%20--%20CPNI%20additional%20Ex-parte%201-31-07.pdf.
[104] *Id.* at 2.

> increase the privacy problems and the likelihood that private information could be misused.[105]

Despite the VON Coalition's argument, the FCC still extended CPNI requirements to VoIP providers in the final rule released April 2, 2007.[106]

The FCC should be commended for extending CPNI rules to VoIP providers. Even though there may be technical differences between telecommunications carriers and VoIP providers, both types of companies are dealing with consumers' personal information. Even though VoIP providers may collect less information, they should still be held to CPNI regulations for the information they do collect. While VoIP providers argue that they take seriously their responsibility to protect consumer privacy,[107] if CPNI rules did not apply to VoIP providers, the providers would be free to change their policies at their convenience, ultimately harming the customer. Bringing VoIP providers under the FCC's umbrella of control will benefit consumer privacy in the long run.

IX. Conclusion

While the Commission has taken great strides in protecting customer privacy, the increasing availability and desirability of customer information compels greater action. Growing societal dependence on mobile devices to store addresses, send e-mail, and schedule daily activities necessitates some form of remedy for the deletion of personal information when these devices are lost, stolen, or simply exchanged for another. The Consumer Coalition proposes the implementation of a hardware-based solution on the manufacturing front, or a software-based solution on the side of the carrier.

---

[105] *Id.* at 4.
[106] Final Rule, *supra* note 19, at 31,950.
[107] VON Letter, *supra* note 102.

In addition, the Consumer Coalition requests that passwords be mandated for all transactions involving a customer account, audit trails log all access to any customer account, and all stored CPNI be encrypted. Further, to fully inform customers of the whereabouts of their CPNI, the Commission should consider a comprehensive opt-in policy that will allow only customers interested in sharing their CPNI to participate in marketing programs. Alternatively, customers should have the right to request disclosure and notification of all entities with which the carrier has shared CPNI. Finally, use of CPNI must be tied to a specific billing or dispute related purpose, and upon expiration of this purpose, the carrier must delete or de-identify this data.

For the reasons stated above, the Consumer Coalition respectfully requests the Commission accept these recommendations to protect the security and privacy of customer data.

Respectfully submitted,

CONSUMER ACTION
CONSUMER FEDERATION OF AMERICA
CONSUMERS UNION
ELECTRONIC PRIVACY INFORMATION CENTER
NATIONAL CONSUMERS LEAGUE
PRIVACY ACTIVISM
PRIVACY JOURNAL
PRIVACY RIGHTS CLEARINGHOUSE
U.S. PUBLIC INTEREST RESEARCH GROUPS
UTILITY CONSUMERS' ACTION NETWORK

MARC ROTENBERG
EXECUTIVE DIRECTOR

MELISSA NGO
SENIOR COUNSEL

ELECTRONIC PRIVACY INFORMATION CENTER

1718 CONNECTICUT AVENUE, N.W., SUITE 200
WASHINGTON, DC 20009
(202) 483-1140