UNFAIR WARNING: BREACH NOTIFICATION IN THE FCC'S ENHANCED TELEPHONE RECORDS SAFEGUARDS

*Stephen L. Markus**

In 2006, news of the ready availability of individuals' private telephone records through online investigation services highlighted the need for privacy regulation to combat pretexting, a practice by which data brokers sought and obtained confidential customer information by fraudulently posing as the target customer. Amid congressional efforts aimed at protecting consumer privacy, the Federal Communications Commission (FCC) implemented heightened restrictions on the disclosure of call records through new regulations for telecommunications carriers. In requiring customer notice of unauthorized phone record disclosures, the new FCC regulations attempt to balance the ultimate goal of consumer protection against the investigative needs of law enforcement entities by prioritizing notice to enforcement agencies upon discovery of a security breach while delaying notice to affected consumers. This Note argues that these delay provisions threaten consumer welfare by needlessly leaving consumers unable to protect themselves against the dangers stemming from such leaks. In lieu of the current FCC breach notification provisions, this Note proposes improving the effectiveness of phone-record breach notification by modeling new regulations or legislation after existing state laws and proposed federal laws for protection of sensitive personal information implicating identity theft.

* B.A., Middlebury College, 2005; J.D. Candidate, 2009, Cornell Law School. I wish to thank the staff of the *Cornell Journal of Law and Public Policy*, particularly Holly McHugh and Julie Tower, for their meticulous editing and helpful comments. I am especially grateful to my family and to Evelyn Israel for their unending patience, love, and support throughout the note-writing process and law school generally.

INTRODUCTION

The public availability of an average citizen's telephone call records, Justice Potter Stewart once noted, "easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[1] The privacy threats of unauthorized phone record disclosure presaged by Justice Stewart gained public attention in the wake of the so-called pretexting scandals reported in 2006.[2] Pretexting occurs when a third party poses as a customer in order to obtain that customer's confidential information, thereby circumventing the carrier's system for protecting billing records. The ease with which a private individual's phone records could be purchased through internet investigation services sent shockwaves through Congress and the telecommunications industry,[3] prompting policymakers to counteract this practice through new legislation and agency regulation.[4]

Section 222 of the Communications Act of 1934 (Section 222) provides statutory authority for regulating the release of telecommunications carriers' customer call records and other personal information, collectively known as "customer proprietary network information" (CPNI).[5] On June 8, 2007, in response to a petition filed by the Electronic Privacy Information Center (EPIC),[6] the Federal Communications Commission

---

[1] Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).

[2] *See, e.g.*, Julie Creswell & Jenny Anderson, *A Company, a Fund and a Feud*, N.Y. TIMES, Nov. 8, 2006, at C1.

[3] *See Combating Pretexting: Hearing on H.R. 936, Prevention of Fraudulent Access to Phone Records Act, Before the H. Comm. on Energy and Commerce*, 110th Cong. 70 (2007) [hereinafter H.R. 936 Hearing] (Prepared Statement of Hon. Steve Largent, President and C.E.O., CTIA—The Wireless Association) ("Incidents like the unauthorized release of General Wesley Clark's call records and the Hewlett-Packard pretexting scandal served as a wake-up call for all of us.").

[4] *See* Matt Richtel, *With a Little Stealth, Just About Anyone Can Get Phone Records*, N.Y. TIMES, Sept. 7, 2006, at C9.

[5] 47 U.S.C. § 222(c) (2000); *see also* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 21 F.C.C.R. 1782, 1784 (proposed Feb. 14, 2006) (notice of proposed rulemaking) ("Practically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting. CPNI therefore includes highly-sensitive personal information.").

[6] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) [hereinafter EPIC Petition].

(FCC) promulgated a new set of regulations accompanying Section 222 in an attempt to bolster the protection of CPNI and broaden the categories of carriers to which the protection applies.[7] The breach notification provisions, inter alia, require that carriers refrain from disclosing a security breach to consumers for at least seven business days after first reporting it to law enforcement officials.[8] This mandate gives law enforcement officials the opportunity to respond to news of a breach before affected consumers are notified.[9] If the breach appears to have an imminent detrimental impact on affected consumers, the new rule grants carriers some discretion in making an exception to the standard procedures.[10] However, law enforcement agencies retain the right to delay notification to consumers for as long as they deem reasonably necessary[11]—a provision that drew objections from two FCC commissioners.[12]

This Note examines the potential impact of the FCC's CPNI breach notification provisions on consumer privacy and welfare. Part I provides background on the laws and policies leading up to the current CPNI rule. Part II analyzes in detail the provisions of the CPNI rule and describes the problematic implications of the FCC's prioritization of notice to law enforcement agencies over notice to consumers in the event of unauthorized disclosure of CPNI. Part III posits that the breach notification procedures contained in existing state (and proposed federal) electronic database protection laws provide superior protection of consumer interests and would form a more effective framework for use in the CPNI context than the procedures in the current FCC rule. The final section concludes.

I. LEGAL AND POLICY BASES FOR TELEPHONE RECORDS PRIVACY LAWS

A. *History of Federal CPNI Protection*

Based upon findings that a citizen's privacy rights are constitutionally protected and are jeopardized by the use of information technology

---

[7] *See* Customer Proprietary Network Information, 72 Fed. Reg. 31,948 (June 8, 2007) (codified at 47 C.F.R. pt. 64). The final CPNI rule went into effect on December 8, 2007. *See* Customer Proprietary Network Information, 72 Fed. Reg. 70,808 (Dec. 13, 2007).

[8] *See* 47 C.F.R. § 64.2011(b)(1) (2008).

[9] *See id.* § 64.2011(a).

[10] *See id.* § 64.2011(b)(2).

[11] *See id.* § 64.2011(b)(3).

[12] *See* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C.R. 6927, 7020 (Apr. 2, 2007) (further notice of proposed rulemaking) (Statement of Commissioner Michael J. Copps); *id.* at 7022 (Statement of Commissioner Jonathan S. Adelstein).

to collect, store, and disseminate personal data,[13] the Privacy Act of 1974 established regulations governing federal agencies' collection and use of personal information about individual citizens.[14] Although it specifically applies to government entities, the Privacy Act has provided the foundation for many other types of privacy legislation.[15] Congress and federal agencies have since enacted a patchwork system of regulations designed to address the privacy threats posed by specific types of industries and business practices.[16]

Restrictions on the disclosure of CPNI in telephone records first appeared in the Telecommunications Act of 1996 (the 1996 Act),[17] which relies upon carriers to protect their customers' personal information through self-regulation. Section 222 of the 1996 Act designated CPNI as a protected category of information and stated that carriers have a duty to safeguard its confidentiality.[18] In the statute, Congress balanced the goals of granting consumers access to their own CPNI with preventing unauthorized disclosure of such information to third parties.[19] Under the accompanying regulations, which are still in effect, a carrier is prohibited from disclosing CPNI to a third party unless it has received the customer's affirmative consent to do so.[20] Expressly delineated requirements for carriers to use in safeguarding CPNI include implementing CPNI-specific training and disciplinary procedures for personnel,[21] maintaining records detailing access to CPNI records,[22] and certifying compliance with the FCC's CPNI requirements.[23] To date, the FCC has brought several enforcement actions against carriers who allegedly failed to meet these requirements.[24]

---

13 *See* Privacy Act of 1974, Pub. L. No. 93-579, §2A, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2000)).

14 *See* 5 U.S.C. § 552a.

15 *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 42.

16 *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2000); Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030 (2000); Electronic Communication Privacy Act of 1986, 18 U.S.C. §§ 2701–2712 (2000); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2000); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2000).

17 Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified in scattered sections of 47 U.S.C. (2000)).

18 *See* 47 U.S.C. § 222(a) (2000).

19 *See* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 21 F.C.C.R. 1782, 1784 (proposed Feb. 14, 2006) (notice of proposed rulemaking).

20 *See* 47 C.F.R. § 64.2005(b) (2008).

21 *See id.* § 64.2009(b).

22 *See id.* § 64.2009(c).

23 *See id.* § 64.2009(e).

24 *See, e.g.*, CBeyond Comm'ns, Inc., 22 F.C.C.R. 18,098 (2007) (forfeiture order); AT&T Inc., 22 F.C.C.R. 16,285 (2007) (order on compliance with the commission's rules and

The 1996 Act's means of protecting CPNI, however, proved unsatisfactory in restricting the availability of consumer phone records through online services.[25] Despite detailed regulations and compliance from carriers, third parties were able to gain unauthorized access to CPNI through pretexting, hacking into customers' online accounts, and possibly through the aid of "dishonest insiders" within the carriers' own ranks.[26] In an effort to curb this access, carriers filed suits against companies offering consumer CPNI for sale, seeking to enjoin such activities.[27] The Gramm-Leach-Bliley Act of 1999 made the unauthorized acquisition of consumer financial information a federal crime, but it did not include CPNI because telephone records are not of a financial nature.[28] The Federal Trade Commission (FTC), utilizing its authority to prevent "unfair or deceptive acts or practices in or affecting commerce," investigated and brought enforcement actions against several purveyors of protected consumer CPNI.[29] State attorneys general also filed suits against alleged pretexters on the basis of state laws.[30] These, however, were indirect means of ensuring the confidentiality of CPNI and did not address the gaps in the underlying system of laws and regulations that enabled such disclosures to occur.

In February 2006, the FCC accepted EPIC's petition for tighter rules on carriers' disclosure of phone records and initiated a rulemaking proceeding, seeking comment on more effective CPNI safeguards.[31] Calling the data brokers' conduct in fraudulently obtaining phone records "disturbing," the FCC asked for detailed information about carriers' CPNI maintenance, security, and disclosure procedures.[32] In April 2007, the FCC adopted new regulations designed to strengthen existing protection of CPNI by restricting the release of "call detail information" (a

---

regulations governing customer proprietary network information); Connect Paging, Inc., 22 F.C.C.R. 15,146 (2007) (forfeiture order).

25 *See* EPIC Petition, *supra* note 6, at 1, Appendix C (listing forty web sites offering to obtain and sell CPNI); *see also* Customer Proprietary Network Information, 72 Fed. Reg. 31,948, 31,949 (June 8, 2007) (codified at 47 C.F.R. pt. 64).

26 *See* EPIC Petition, *supra* note 6, at 1.

27 *See* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C.R. 6927, 6934–35 (Apr. 2, 2007) (further notice of proposed rulemaking) [hereinafter CPNI NPRM (Apr. 2, 2007)].

28 *See* 15 U.S.C. § 6821 (2000).

29 *Id.* § 45(a)(2); *see* H.R. 936 Hearing, *supra* note 3, at 32 (Statement of Lydia Parnes, Federal Trade Commission).

30 *See* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 6935.

31 *See* Customer Proprietary Network Information, 71 Fed. Reg. 13,317, 13,318 (Mar. 15, 2006) (codified at 47 C.F.R. pt. 64).

32 *Id.*

subset of CPNI),[33] notifying customers of account changes,[34] specifying requirements for notifying law enforcement officials and customers of unauthorized disclosure of CPNI,[35] and establishing a "general requirement to take reasonable measures to discover and protect against activity that is indicative of pretexting."[36] These provisions form the primary subject of this Note and will be discussed in detail below.[37]

While the FCC was engaged in the rulemaking process, widely publicized accounts of pretexting prompted Congress to implement protective measures as well. In January 2006, reports surfaced detailing how a blogger was able to successfully purchase General Wesley Clark's cell phone records through an online data broker.[38] In September 2006, the news broke that private investigators, hired by Hewlett-Packard to identify the source of a leak, obtained the phone records of both the corporation's board members and journalists in the course of their investigation.[39] In the wake of the resulting public outcry over the availability of consumer phone records, Congress eliminated the gap in federal law regarding pretexting by criminalizing fraudulent methods of obtaining confidential phone records.[40] The passage of the Telephone Records and Privacy Protection Act of 2006 gave law enforcement agencies stronger tools for curtailing the practices of pretexters and other data brokers offering phone records for purchase, but some members of Congress thought that additional statutory safeguards were necessary.[41]

---

33 Customer Proprietary Network Information, 72 Fed. Reg. 31,948, 31,961 (June 8, 2007) (codified at 47 C.F.R. pt. 64) ("Call detail information . . . [is][a]ny information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call."); *see also* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 6936 (prohibiting carriers from releasing call detail information based on customer-initiated telephone contact unless the customer provides the carrier with a pre-established password, unless the customer requests call detail information to the customer's address of record, and unless a carrier chooses to disclose non-call-detail CPNI to a customer after the carrier authenticates the customer).

34 *See* Customer Proprietary Network Information, 72 Fed. Reg. at 31,949 (finding that "this notification requirement will also empower customers to provide carriers with timely information about pretexting activity, which the carriers may not be able to identify easily"); *see also* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 6942 (requiring carriers to notify customers immediately of certain account changes).

35 *See* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 6943.

36 *Id.* at 6946.

37 *See infra* Part II.A.

38 *See* Frank Main, *Blogger Buys Presidential Candidate's Call List: 'Nobody's Records Are Untouchable,' as $90 Purchase Online Shows*, CHI. SUN-TIMES, Jan. 13, 2006, at A10.

39 *See* Richtel, *supra* note 4, at C9.

40 *See* Telephone Records and Privacy Protection Act, 18 U.S.C.A. § 1039 (West 2007).

41 See *infra* Part I.B. for a description of proposed federal legislation to regulate unauthorized access to CPNI.

B. Proposed Federal CPNI Legislation

The proposed Prevention of Fraudulent Access to Phone Records Act of 2007 (H.R. 936) contains additional measures designed to bolster CPNI protection.[42] The bill would prohibit the third-party solicitation of another person or business to obtain an individual's CPNI if the soliciting third party should know that the records would be sought under false pretenses.[43] A violator of this provision would be subject to an enforcement action by the FTC.[44] H.R. 936 would require the FCC to enforce amendments to Section 222 further restricting third-party CPNI access to certain situations, some of which mirror those contained in the FCC's subsequently adopted 2007 CPNI rule.[45] However, H.R. 936 goes beyond the scope of the FCC's CPNI rule by requiring more direct FCC involvement in the ongoing enforcement process. A carrier that discovers a breach would be required by H.R. 936 to notify affected customers and report the breach to the FCC, rather than to law enforcement officials.[46] Additionally, the FCC would be tasked with conducting "periodic audits" to ensure compliance with CPNI confidentiality regulations.[47] Although these procedures would impose greater maintenance and enforcement requirements upon the FCC, they might also ensure more effective oversight and accountability by giving federal regulators, rather than carriers, the discretion to determine the timing of notification to consumers.

Similarly, the Protecting Consumer Phone Records Act (S. 780) proposes amending Section 222 to tighten restrictions on the disclosure of CPNI and to specify procedures for notifying consumers of system breaches.[48] Like H.R. 936, S. 780 bars not only unauthorized acquisition of another's phone records, but also solicitation of phone records from a party whom one knows will use unlawful means to obtain them.[49] In the event of a disclosure to a third party in violation of S. 780, providers would be required to notify affected consumers within fourteen days of discovery of such a breach, subject to delays if law enforcement or national security agencies deem them necessary.[50] Significantly, in addition to delegating enforcement duties to the FCC, the FTC, and to the states, S. 780 explicitly grants a private right of action to both providers

---

42 *See* Prevention of Fraudulent Access to Phone Records Act, H.R. 936, 110th Cong. (2007).

43 *See id.* § 101(b).

44 *See id.* § 103.

45 *See id.* § 203.

46 *See id.* § 203(h)(1)(A).

47 *Id.*

48 *See* Protecting Consumer Phone Records Act, S. 780, 110th Cong. (2007).

49 *See id.* § 2(a).

50 *See id.* § 509(d).

and consumers who fall victim to unauthorized access of CPNI.[51] The advantages of this model lie in its multiple avenues of enforcement and in its straightforward procedures for consumer notification, except in cases where law enforcement agencies find delay necessary. Problems may arise, however, because S. 780 allows providers, of their own accord, to delay notification of consumers for fourteen days after discovery of the breach, when discovery itself may not occur until the disclosure has already begun to pose real risks for consumers.[52]

II. THE FCC'S STRENGTHENED CPNI RULE

A. Prioritized Breach Notification to Law Enforcement

The FCC's newly effective CPNI rule of 2007 provides that in the event of an unauthorized disclosure of protected CPNI—for instance, if a carrier discovers that call records have been improperly disclosed—a carrier must notify the United States Secret Service and the Federal Bureau of Investigation "[a]s soon as practicable," and no later than seven business days after "reasonable determination" of the breach.[53] A carrier may not notify affected consumers or the general public until it has completed its notice to law enforcement in accordance with the rule's procedures.[54] Generally, a carrier must wait seven business days after its notice to law enforcement before it notifies consumers.[55] However, if the carrier perceives "an extraordinarily urgent need" to notify affected consumers earlier than the customary seven-day waiting period "in order to avoid immediate and irreparable harm," the rule requires the carrier to indicate this need to the law enforcement agencies and to first consult with the relevant agency before initiating consumer notification.[56] Another exception to the standard notification timeline allows an investigating agency to further delay notice to consumers or the public for an initial period of up to thirty days—subject to extension "as reasonably necessary in the judgment of the agency"—if it determines that notice per the ordinary procedures "would impede or compromise an ongoing or potential criminal investigation or national security."[57] The rule also gives carriers considerable latitude in customizing the method of consumer breach notification to accord with their own judgments in light of specific circumstances.[58]

---

51 *See id.* § 2(c)–(d).
52 *See id.* § 4(d)(2).
53 47 C.F.R. § 64.2011(b) (2008).
54 *See id.* § 64.2011(a).
55 *See id.* § 64.2011(b)(1).
56 *Id.* § 64.2011(b)(2).
57 *Id.* § 64.2011(b)(3).
58 *See* Customer Proprietary Network Information, 72 Fed. Reg. 31,948, 31,950 (June 8, 2007) (codified at 47 C.F.R. pt. 64).

The FCC frames its objective in adopting the new CPNI regulations as promoting consumer protection.[59] However, in practice, provisions requiring immediate notice to law enforcement agencies—alongside delayed notification to consumers—reserve for law enforcement officials and carriers the discretion to determine when and how to notify affected consumers. Meanwhile, the consumers at risk of adverse action remain unaware of the breach. The result is that affected consumers cannot immediately take individualized steps to mitigate the risks posed by such disclosures of their sensitive information. The FCC claims that its rule balances "a customer's need to know with law enforcement's ability to undertake an investigation of suspected criminal activity, which itself might advance the goal of consumer protection."[60] It advances two reasons in support of this compromise: (1) immediate public knowledge of a breach may hinder the investigation efforts of law enforcement officials, and (2) the delay is reasonable when considered in conjunction with the rule's exception enabling immediate notice if the carrier anticipates a risk of "immediate and irreparable harm."[61]

The FCC's stated reasons for delayed notice to consumers, while sensible on their face, fail to justify a rule that defers to the judgment of carriers in determining the nature and timing of consumer notification. First, the concern for effective law enforcement and national security does not justify a system of delayed notification absent extraordinary circumstances. In effect, this rule presumes that threats requiring secrecy are the norm, instead of the exception. This presumption departs from immediate notice provisions in other data protection laws designed to combat invasive practices whose methods and threats largely mirror those of telephone record pretexting.[62] Dissenting with respect to this provision in the final CPNI rule, FCC Commissioner Michael J. Copps called this delayed notice requirement "needlessly overbroad."[63] The interest in ensuring law enforcement efficacy could be just as effectively protected by allowing immediate notice to consumers as soon as law enforcement agencies receive news of a breach, unless the investigating agency decides to affirmatively invoke an exception providing for de-

---

59 *See* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C.R. 6927, 6933 (Apr. 2, 2007) (further notice of proposed rulemaking) [hereinafter CPNI NPRM (Apr. 2, 2007)] ("The carriers' record on protecting CPNI demonstrates that the Commission must take additional steps to protect customers from carriers that have failed to adequately protect CPNI.").

60 Customer Proprietary Network Information, 72 Fed. Reg. at 31,950.

61 *See* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 6944.

62 *See infra* text accompanying notes 99–105.

63 CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 7020 ("[The rule] fails to distinguish those exigent circumstances in which delayed notification is necessary from what I believe to be the majority of cases in which immediate notification to a victim is appropriate.").

lay.[64] Additionally, Commissioner Copps perceptively noted that contrary to the Commission's stated assumptions, immediate notification to affected consumers may actually *improve* the success of an investigation by enabling consumers to work together with law enforcement in identifying the perpetrators of the breach or third parties utilizing the leaked CPNI.[65]

Second, the grant of discretion to carriers to expedite consumer notification under compelling circumstances does little to ensure reliable protection of CPNI. An initial problem is that carriers, despite their possible expertise regarding the best means of protecting CPNI stored in their customer databases, are not experts on the practical implications of a CPNI breach for customer privacy.[66] Therefore, it makes little sense to entrust carriers with the fundamental decision of whether expedited notice to consumers is necessary in a particular instance. Even though market considerations will presumably encourage carriers to act in their customers' best interest, carriers may instead succumb to the countervailing desire to minimize controversy by ignoring, delaying acknowledgment of, or downplaying the significance of a newly discovered breach.[67] At the very least, the FCC, with its broad expertise in this area and its greater levels of accountability, could more effectively assume this responsibility. For a more sensible method of responding to a suspected breach, the FCC might look to its own new regulation on notification of account changes, a provision which requires immediate notification to consumers in the event of a change to existing account information or the creation of new account information.[68]

---

64 *See* Comments of Consumer Action, et al., *In re* Further Notice of Proposed Rulemaking: Customer Proprietary Network Information, 21 (July 9, 2007) (No. CC 96-115) ("[A]ll 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. In addition, such circumstances must truly be exigent, and the harm of disclosure 'immediate and irreparable,' as customers have a right to protect their own data and act upon notification of a breach.").

65 *See* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 7020 ("I continue to believe that notification to the victim . . . will often actually aid law enforcement because the violator is frequently someone well known to the victim. If an unauthorized individual has gained access to personal telephone records involving victims of stalking or spousal violence, it won't be the carrier or the law enforcement agency—but the victims—who are in the best position to know when and how harm may be heading toward them.").

66 *See id.*

67 Paul M. Schwartz and Edward J. Janger term this phenomenon the "disclosure disincentive." Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 928 (2007) ("Disclosure may increase the risk of liability, because it makes traceable an otherwise untraceable security breach. Furthermore, disclosure also brings publicity to an event and might thereby prompt costly legal action or regulatory scrutiny.").

68 *See* Customer Proprietary Network Information, 72 Fed. Reg. 31,948, 31,949 (June 8, 2007) (codified at 47 C.F.R. pt. 64) ("[T]he Commission finds that this notification require-

Third, under the new CPNI regulations, the ability of carriers to protect the privacy of their consumers by circumventing the customary waiting period is still subject to de facto approval by federal law enforcement agencies. The CPNI rule might permit an investigating agency to indefinitely withhold consumer notification on the unsupported grounds that extension of the initial waiting period is "reasonably necessary in the judgment of the agency."[69] The prudence that agencies such as the Federal Bureau of Investigation and the National Security Agency have demonstrated in the handling of private consumer information has recently been called into question by the controversies surrounding federal law enforcement's warrantless surveillance program, a process that in part involved CPNI.[70] Law enforcement agencies often insulate themselves from accountability by justifying any action taken as necessary to national security. Thus, enabling law enforcement officials to indefinitely delay notification to consumers of a breach that may pose an imminent and detrimental threat to their welfare[71] potentially opens the door to abuses in discretion for which law enforcement privileges obstruct judicial oversight.[72]

Under the new regulatory system, the very nature of the FCC's own enforcement measures may further undermine proper notification of consumers whose CPNI has been compromised. The CPNI rule places the onus on carriers to discover and report CPNI leaks to law enforcement and affected consumers, based on the 1996 Act's statutory mandate that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information."[73] However, upon learning of a CPNI

---

ment will also empower customers to provide carriers with timely information about pretexting activity, which the carriers may not be able to identify easily.").

69 47 C.F.R. § 64.2011(b)(3) (2008); *see also* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 7022–23 (Statement of Commissioner Jonathan S. Adelstein) ("I find no statutory basis in the Act for granting the FBI a blank check to delay notice to customers. I can understand the need for delay in extraordinary circumstances identified by law enforcement, but automatic delays coupled with unlimited and unchecked extensions are not appropriate.").

70 *See* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 7021; *see also* Frederick M. Joyce & Andrew E. Bigart, *Liability for All, Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 VAL. U. L. REV. 1481, 1493 (2007).

71 Congress has recognized that "the unauthorized disclosure of telephone records not only assaults individual privacy but, in some instances, may further acts of domestic violence or stalking, [and] compromise the personal safety of . . . victims of crime . . . ." Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, § 2, 120 Stat. 3568, 3568 (2007) (codified at 18 U.S.C. § 1039). *See also* Prevention of Fraudulent Access to Phone Records Act, H.R. 936, 110th Cong. § 201(4) (2007) ("Disclosure of personal records can also lead to harassment, intimidation, physical harm, and identity theft.").

72 *See, e.g.*, Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 917 (N.D. Ill. 2006) (finding customers' discovery request that a carrier disclose whether or not it had provided large quantities of detailed consumer call records to the National Security Administration to be barred by the state secrets privilege based on national security concerns).

73 47 U.S.C. § 222(a) (2000); *see* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 6943.

breach caused by a carrier's disclosure, the FCC may assume that the carrier's CPNI safeguards are systemically inadequate[74] and may proceed to punish the carrier.[75] Rewarding such self-policing diligence with a presumption of faulty procedures and the threat of enforcement sanctions threatens to deter adherence to the procedural foundation upon which the CPNI protection model relies.[76] Carriers who properly identify and report weaknesses in their CPNI safeguarding systems risk exposing themselves to further regulatory intervention, while those who do not may escape liability for their errors.[77] Such a reporting disincentive may in fact delay notification of a breach to affected consumers or even prevent it altogether. In all, the prescribed means of enforcing the new CPNI provisions detract from the ultimate goal of protecting the privacy of consumer phone records.

B. Risks of Delayed Notice to Consumers

Requiring carriers to notify consumers of a suspected breach is necessary to ensure that affected consumers take appropriate protective measures upon learning that their private calling information has been compromised.[78] The FCC asserts that its new regulations are consistent with this interest.[79] However, as discussed above, the breach notification provisions contained in the CPNI regulations have the potential to undermine the FCC's own stated objective by delaying notification to victims of pretexting in order to protect law enforcement and national security objectives.[80] Delayed notice to consumers is dangerous because the moment of the initial breach is when notice to consumers is most crucial in

---

74 *See* Customer Proprietary Network Information, 72 Fed. Reg. at 31,950 ("[T]he Commission hereby puts carriers on notice that the Commission henceforth will infer from evidence that a pretexter has obtained unauthorized access to a customer's CPNI that the carrier did not sufficiently protect that customer's CPNI.").

75 *See id.* at 31,951.

76 *See* Comments of the National Telecommunications Cooperative Association, et al., *In re* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information, 3 (Aug. 7, 2007) (No. CC 96-115) ("There is no reason to infer that a carrier has not satisfied its legal obligation to take 'reasonable measures' to protect CPNI simply because a pretexter is successful in its efforts.").

77 *See* Schwartz & Janger, *supra* note 67, at 928.

78 Without the benefit of such a requirement, consumers in the past have typically failed to learn of breaches for a substantial period of time. *See, e.g.*, *Internet Data Brokers: Who Has Access to Your Private Records?: Hearing Before the Subcomm. on Oversight and Investigations of the Comm. on Energy and Commerce*, 109th Cong. 19 (2006) (statement of Adam Yuzuk of Atlantic Beach, New York).

79 *See* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C.R. 6927, 6944 (Apr. 2, 2007) (further notice of proposed rulemaking) ("This notice will also empower carriers and consumers to take whatever 'next steps' are appropriate in light of the customer's particular situation.").

80 *See supra* notes 59–72 and accompanying text.

order to prevent harm from the unauthorized disclosure of their telephone records.[81] Victims of CPNI breaches who, because of delayed notice or otherwise, lack the ability to take affirmative protective measures, face potentially serious threats to their privacy and safety.[82] Consumers with compromised CPNI face a heightened risk of harassment and violence to their person. Documented intrusions on privacy from past breaches have included incidents of stalking and physical threats.[83] One data broker's sale of the home phone numbers and addresses of Los Angeles Police Department detectives to suspected mobsters resulted in the intimidation of the detectives and their families.[84] In another case, a woman was murdered by a stalker who had purchased her social security number, date of birth, and employment address from a private investigator who obtained the information by posing as an insurance company official.[85]

Although dismissed by some as improbable,[86] withheld or delayed notice to consumers increases the potential for identity theft, given the similarity of methods by which pretexters obtain CPNI and the personal information used to steal a person's identity.[87] Additionally, once an unauthorized party obtains telephone records, the subject of the records is at increased risk of other intrusions on personal and financial privacy.[88] Congress has recognized the severity of the risk to individuals posed by the misuse of such data.[89]

---

81 *See* CPNI NPRM (Apr. 2, 2007), 22 F.C.C.R. at 7023 (Statement of Commissioner Jonathan S. Adelstein).

82 *See supra* note 71.

83 *See, e.g.*, *Phone Records for Sale: Why Aren't Phone Records Safe from Pretexting?: Hearing Before the Comm. on Energy and Commerce of the House of Representatives*, 109th Cong. 46 (2006) [hereinafter *Phone Records for Sale*] (Prepared Statement of Hon. Jon Leibowitz, Commissioner, Federal Trade Commission) ("Although the acquisition of telephone records does not present the opportunity for immediate financial harm as the acquisition of financial records does, it nonetheless is a serious intrusion into consumers' privacy and could result in stalking, harassment, and embarrassment.").

84 *Id.*

85 Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1005–06 (N.H. 2003).

86 *See Phone Records for Sale*, *supra* note 83, at 46.

87 *Protecting Consumers' Phone Records: Hearing Before the Subcomm. on Consumer Affairs, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 35 (2006) (Prepared Statement of Robert Douglas, Chief Executive Officer, PrivacyToday.com).

88 *See* Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, § 2, 120 Stat. 3568, 3568 (2007) (codified at 18 U.S.C. § 1039).

89 *See* Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. § 2(8) (2007) (finding that "data misuse and use of inaccurate data have the potential to cause serious or irreparable harm to an individual's livelihood, privacy, and liberty and undermine efficient and effective government operations").

III. DATA BREACH NOTIFICATION LAWS: SUPERIOR PROTECTION OF CONSUMER PRIVACY

A. State Provisions

In developing more effective regulation of CPNI breach notification procedures, the FCC should look to state laws responding to breaches of sensitive personal data. Sparked in large part by news of database security breaches[90] that compromised large quantities of consumers' "personal information"[91] and made consumers vulnerable to identity theft, the majority of states enacted laws requiring private entities whose databases are involved in a security breach to notify affected individuals.[92] The basic purpose of such provisions is to reduce the risk of identity theft or fraud by enabling consumers to monitor their credit histories.[93] The first state to pass such a law was California in 2003, and its statute serves as the model on which other states have based their respective data breach notification laws.[94] Notably, California's notification requirements induced the information broker ChoicePoint to notify at least 166,000 affected consumers of one of the first major breaches of personal information.[95]

---

90 For a comprehensive list of reported database breaches, see Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Dec. 29, 2008).

91 Most states with data breach notification laws follow California's lead in defining the "personal information" covered by their respective statutes as an "individual's first name or first initial and last name in combination with any one of the following data elements, when either the name or the data elements are not encrypted": (1) social security number; (2) driver's license number or state ID card number; and (3) account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. CAL. CIV. CODE § 1798.82(e) (West 2007); *see also, e.g.*, ARIZ. REV. STAT. § 44-7501(L)(6) (West 2008). However, under the California definition, "personal information" subject to notification requirements does not include publicly available information that is lawfully available to the general public from federal, state, or local government records. *See id.* § 1798.82(f).

92 As of December 16, 2008, 44 states, the District of Columbia, Puerto Rico, and the Virgin Islands had enacted laws requiring consumer notification in the event of a breach of personal information. *See* National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Dec. 29, 2008). For an overview of each state's provisions, see Consumers Union, States with Notice of Security Breach Laws, at http://www.consumersunion.org/campaigns//financialprivacynow/002215indiv.html (last visited Dec. 29, 2008).

93 *See* Federal Trade Commission, Dealing with a Data Breach, http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html (last visited Dec. 29, 2008).

94 *See* Daniel J. Solove et al., INFORMATION PRIVACY LAW 673, 699 (2d ed. 2006); *see also* CAL. CIV. CODE § 1798.81.5–.84.

95 *See* Jon Swartz & Byron Acohido, *Who's Guarding Your Data in the Cybervault?: ChoicePoint Redeemed Itself, but Not All Brokers as Careful*, USA TODAY, Apr. 2, 2007, at 1B. Although ChoicePoint discovered the breach in October of 2004, it delayed notification to the over 30,000 California victims until February of 2005 in order to minimize interference with the law enforcement investigation. *See* Solove et al., *supra* note 94, at 699. In response to the ensuing outcry from other states and members of the public, ChoicePoint voluntarily

Under these laws, an entity discovering a breach must notify consumers and law enforcement officials according to the procedures of each state in which an affected individual resides. The state laws are divided on whether a notification-triggering breach occurs merely as the result of an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information"[96] or whether there must also exist a "reasonable likelihood of harm to customers" before notification is required.[97] Enforcement methods and penalties for noncompliance also vary widely from state to state.[98] In most other significant aspects, however, the state laws have common provisions that would more effectively protect consumer privacy in the telephone record context than the notification procedures in the FCC's CPNI rule.

The time frame for data breach notification required by most state provisions better incorporates the urgency necessary to minimize adverse effects of unauthorized CPNI disclosure than the current FCC rule does. Most state provisions require disclosure of the breach to each affected individual as expediently as possible and without unreasonable delay,[99] but some states make allowances for special circumstances, such as the needs of law enforcement,[100] or any other measures necessary to determine the scope of the breach and restore the integrity and security of the data system.[101] A few states mirror the FCC's CPNI rule in requiring notice to law enforcement prior to individual consumer notice.[102] The CPNI rule, however, departs from the majority of state notification provisions by automatically delaying notification by a set period of seven business days after notification to law enforcement, a process which itself is allotted up to seven additional business days.[103] This delay must occur unless a carrier perceives "an extraordinarily urgent need" to notify con-

---

decided to notify all remaining individuals whose information was affected by the breach. *See id.* at 699–700.

96 CAL. CIV. CODE § 1798.82(d) (West 2008).

97 ARK. CODE ANN. § 4-110-105(d) (West 2007).

98 *E.g.*, *compare* ARIZ. REV. STAT. § 44-7501(H) (West 2008) (providing for enforcement only by the state attorney general, who may bring an action for actual damages plus a civil penalty of ten thousand dollars per breach), *with* WASH. REV. CODE ANN. § 19.255.010(10)(a) (West 2007) (allowing any customer injured by a violation of the breach notification law to bring a civil action to recover damages).

99 *See, e.g.*, WASH. REV. CODE ANN. § 19.255.010(1).

100 *See, e.g.*, CAL. CIV. CODE § 1798.82(a).

101 *See, e.g.*, 815 ILL. COMP. STAT. ANN. § 530/10(a) (West 2007). A few states additionally mandate that such notice be provided no later than 45 days after discovery of the breach. *See, e.g.*, FLA. STAT. ANN. § 817.5681(1)(a) (West 2007). Wisconsin, however, requires only that an entity notify individuals whose information was affected by a breach within 45 business days after discovery of the breach. *See* WIS. STAT. ANN. § 895.507(3)(a) (West 2007).

102 *See, e.g.*, N.J. STAT. ANN. § 56:8-163(c)(1) (West 2007).

103 *See* 47 C.F.R. § 64.2011(b), (b)(1) (2008).

sumers "in order to avoid immediate and irreparable harm."[104] In that case, the carrier may notify consumers only after consultation with the relevant investigating agency.[105]

This system tends to unnecessarily withhold information from affected individuals, who remain unaware of the breach and thus unable to take necessary measures to ensure the safety of themselves and other parties. Although some delay should logically be allowed in order to enable a carrier to determine the scope of a breach, to prevent further unauthorized disclosures, and to report the breach to law enforcement, notifying the consumer as soon as possible after the completion of these actions allows the consumer to mitigate the damage of identity theft or other possible harm.[106] As such, a carrier should at the very least be allowed to notify affected individuals in an expedient manner unless law enforcement specifically requests a delay.[107]

The methods of notification included in the majority of state data breach notification laws would be preferable to the current CPNI policy because they set baseline standards for the form and content of the notification process to ensure that individuals receive adequate notice of breaches. Most states have modeled their notification form requirements after California's,[108] which allows for written notice, electronic notice, or various forms of "substitute notice" for occasions when the former methods would be impracticable due to high cost, large quantities of affected individuals, or insufficient contact information.[109] Some states also permit telephonic notice.[110] A few states, including North Carolina, have set minimum requirements for the content of the notice.[111] The FCC's CPNI rule declines to adopt any of these standards; instead, it grants leeway to the carriers to tailor their notification methods according to their own preferences and capacities, or to meet the exigencies of a par-

---

104 *Id.* § 64.2011(b)(2).

105 *Id.*

106 *See* CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS, OFFICE OF PRIVACY PROTECTION, RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 11 (Feb. 2007), *available at* http://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/PrivacyProtection.pdf.

107 *See id.*

108 *See, e.g.*, N.C. GEN. STAT. ANN. § 75-65(e) (West 2007).

109 CAL. CIV. CODE § 1798.82(b) (West 2008). "Substitute notice" is usually defined to require all of the following: (1) e-mail notice, (2) conspicuous posting on the breaching party's website (if any), and (3) notification to major statewide media. *Id.*

110 *E.g.*, N.C. GEN. STAT. ANN. § 75-65(e)(3).

111 *See, e.g.*, *id.* § 75-65(d) (requiring descriptions of (1) the incident, (2) the type of personal information that was subject to unauthorized access, (3) the general acts of the business to protect the information from further unauthorized access, (4) a phone number that the consumer may call for further information and assistance, and (5) advice that directs the consumer to review account statements and credit reports).

ticular situation.[112] While such flexibility might simplify compliance from a carrier's standpoint, it may also permit methods of notice that do not effectively reach the intended recipients.[113] For example, under this system, a carrier might opt to notify affected customers merely by posting a notice on the carrier's website. A more mutually advantageous approach would be to follow most states by (1) establishing baseline notification methods and (2) finding a carrier to be compliant if it notifies consumers in accordance with the established baseline methods in the event of a breach.[114]

Finally, the exceptions to the standard procedures contained in the state breach notification laws better accord with consumer interests than those in the FCC's CPNI rule, because the notification priorities of the state provisions emphasize the privacy interests of consumers over the investigative concerns of law enforcement. Most states require expedient notice to consumers unless law enforcement affirmatively requests a delay.[115] In contrast, the CPNI rule mandates a presumption of delayed notice unless carriers inform law enforcement officials of an extraordinary risk of harm requiring immediate consumer notice.[116] This provision of the CPNI rule is problematic because telephone carriers are not experts on consumer welfare, making it extremely unlikely that they could accurately predict and distinguish the individualized risks attending one CPNI breach versus another. The state data breach notification approach to law enforcement coordination is supported in the CPNI context by FCC Commissioner Copps and multiple consumer interest groups, because it enables law enforcement to conduct a prioritized investigation if necessary while also preserving expedient notice to the consumers affected by a breach.[117]

B. Proposed Federal Provisions

In an effort to eliminate the difficulties of compliance with the patchwork system of state data breach disclosure laws currently in force, lawmakers in the 110th Congress introduced several pieces of legislation aimed at simplifying and streamlining a private, personal information holder's response to a newly discovered security breach.[118] The various

---

112 *See* Consumer Proprietary Network Information, 72 Fed. Reg. 31,948, 31,948, 31,950 (June 8, 2007) (codified at 47 C.F.R. pt. 64).

113 *See* Schwartz & Janger, *supra* note 67, at 952 (discussing consumer perceptions of "triviality" based on junk-mail-like form and confusing content of past data breach notices).

114 *See, e.g.*, CAL. CIV. CODE § 1798.82(h).

115 *See, e.g.*, *id.* §§ 1798.29(c), 1798.82(c) (allowing for delayed notice if a law enforcement agency determines that timely notification would impede a criminal investigation).

116 *See* 47 C.F.R. § 64.2011(b)(2) (2008).

117 *See supra* notes 62–65 and accompanying text.

118 *See* Privacy and Cybercrime Enforcement Act of 2007, H.R. 4175, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); Data Security Act

bills in large part borrow provisions from state data breach laws. The proposed notification provisions, even if not ultimately passed into law, could provide a more effective framework for CPNI breach notification than the requirements of the current FCC rule.

The proposed federal data breach notification laws rightfully require notice in a more expeditious and practical fashion than the FCC's CPNI rule. Like some of the state laws, the proposed bills are more limited than California's data breach notification law, as they require notice only upon discovery of unauthorized access to personal information that is reasonably believed to pose a threat to consumers' financial security.[119] Given the centrality of this determination to whether notification occurs, the more ideal bills mandate law enforcement review of an entity's "risk assessment."[120] The bills also uniformly endorse the expediency requirements for consumer notification found in the state laws, eschewing the automatic delay of the CPNI rule.[121] Where law enforcement officials deem a delay in notice necessary to ensure the efficacy of a criminal investigation, they may obtain a limited delay upon written request to the entity.[122] This insistence on timely notice to the extent practicable is fundamental to ensuring that consumers at risk of identity theft have the opportunity to monitor their credit reports and remain vigilant for fraud, while consumers subject to a CPNI breach can take customized preventative action based on the content of the information disclosed. Additionally, the bills follow North Carolina's example in setting forth standards

---

of 2007, S. 1260, 110th Cong. (2007); Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007); Identity Theft Prevention Act, S. 1178, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007).

119 *See, e.g.*, S. 1202 § 2(2)(B). The Consumers Union has voiced its concern regarding the subjective assessment of risk that such notice-triggers require. *See* Letter from Gail Hillebrand, Financial Services Campaign Leader, Consumers Union, to Hon. Mark Pryor, Chair of Commerce Subcommittee on Consumer Affairs, Insurance, and Automotive Safety, U.S. Senate (Apr. 24, 2007) (on file with Consumers Union), *available at* http://www.consumersunion.org/pdf/S1178.pdf ("We are deeply concerned that tying notice to an affirmative determination of risk will excuse notice in that most common of circumstances where there is simply not enough information to determine the level or nature of the risk due to incomplete information.").

120 *E.g.*, S. 239 § 3(b)(1) (providing safe harbor from the notice requirements if an entity's risk assessment concludes there is no significant risk of harm to individuals, the entity notifies the United States Secret Service of its conclusion, and the Secret Service does not indicate that notice should be given).

121 *See, e.g.*, S. 495 §§ 311(c)(1)–(2) (requiring notice "without unreasonable delay following the discovery . . . of a security breach" where "reasonable delay" may include "any time necessary to determine the scope of the security breach, prevent further disclosures, and restore the reasonable integrity of the data system and provide notice to law enforcement when required").

122 *See* S. 239 § 2(d)(1). Other bills expand this law enforcement delay for purposes of civil investigations and national security. *See, e.g.*, S. 1178 § 3(e)(2).

for both the form and content of the notice to be provided.[123] Such basic standards should be integrated into the CPNI rule—which in its current state "leaves carriers the discretion to tailor the language and method of notification to the circumstances"[124]—to better ensure that consumers actually receive notice by a means that captures their attention, imparts the significance of the breach, and includes resources for assistance or additional information.

Enforcement obligations in the proposed data breach notification bills vary but fall primarily to the federal and state attorneys general. This scheme allows for a greater level of oversight than the CPNI rule's reliance on the FCC for enforcement.[125] Like the data security bills, some of the proposed federal CPNI laws attempt to broaden enforcement of CPNI regulation beyond the FCC by extending enforcement authority to the states, while leaving breach notification requirements enforceable only by the FCC.[126] Enabling state enforcement of the CPNI breach notification rule would likely improve carriers' compliance with the provisions by subjecting them to more stringent means of oversight than accountability to the FCC alone. An even more advantageous approach might entail delegating responsibility to a third party supervisory agent to work directly with private information holders in coordinating their responses to newly discovered breaches and in monitoring the effectiveness of consumer notification.[127]

Like the existing state laws, the proposed federal data breach notification laws represent a superior model for ensuring effective consumer notice of CPNI breaches because of their insistence on timely, effective, and practical notice. While the FCC's CPNI rule presumes the necessity of prioritized notice to law enforcement, other proposed federal laws reverse the presumption in favor of consumers by requiring an affirmative determination of risk by law enforcement before an agency may delay consumer notification.[128] The federal data breach notification bills better balance the interests of consumers with the needs of law enforcement by allowing limited notification delays only when the relevant officials deem such delays to be necessary.[129] The inherent distinctions between personal information and CPNI should not militate against adopting sim-

---

123 *See, e.g.*, S. 1260 §§ 4(c)–(d).

124 Customer Proprietary Network Information, 72 Fed. Reg. 31,948, 31,950 (June 8, 2007) (codified at 47 C.F.R. pt. 64).

125 *See, e.g.*, S. 239 §§ 8–9. *But see* S. 1260 § 5 (providing for enforcement by various administrative entities).

126 *See, e.g.*, Protecting Consumer Phone Records Act, S. 780, 110th Cong. § 7 (2007).

127 *See* Schwartz & Janger, *supra* note 67, at 960.

128 *See* Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. §§ 2(a), 2(d) (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. §§ 311–12 (2007).

129 *See supra* note 122.

ilar procedures for notifying affected consumers of system breaches of either kind of information.[130]

CONCLUSION

Telephone records are at the heart of the broader societal debate about consumer privacy in today's information age.[131] At a time when private businesses record and keep a significant portion of personal activities in electronic databases, regulation of the maintenance and dissemination of sensitive consumer information is an essential step in the right direction, but it alone is not enough to safeguard consumer privacy.[132] As many individual states have found, disclosing news of a database breach of personal information to affected consumers by the most expedient means available best allows consumers to take protective action, thus mitigating the risk and expense of identity theft and financial fraud.[133] In the case of telephone records, prompt and meaningful notification of unauthorized disclosure should be even more fundamental because of the unique threat to a person's physical safety posed by the person who obtained the sensitive information.[134] Furthermore, immediate consumer notification in the CPNI context enables affected consumers to assist in the investigation of the circumstances surrounding the breach, thus making it more likely that the perpetrator will be discovered.[135] Given the sensitivity of CPNI currently vulnerable to unauthorized disclosure, Congress would better protect consumer welfare by strengthening the FCC's recently adopted CPNI breach notification standards.

---

130 *See* Protecting Consumer Phone Records Act, S. 780, 110th Cong. § 3(a) (2007) (proposing that the FCC adopt CPNI regulations "similar in scope and structure" to the FTC's regulations implementing the Gramm-Leach-Bliley Act's protection of financial information, "taking into consideration the differences between financial information and customer proprietary network information").

131 *See* Jerry Berman, *Security, Privacy, and Government Access to Commercial Data*, *in* PROTECTING WHAT MATTERS: TECHNOLOGY, SECURITY, AND LIBERTY SINCE 9/11, at 100, 103 (Clayton Northouse ed., 2006).

132 *See* Chris Jay Hoofnagle, *Privacy Self-Regulation: A Decade of Disappointment*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 379, 393 (Jane K. Winn ed., 2006).

133 *See* Federal Trade Commission, *supra* note 93.

134 *See supra* note 71.

135 *See* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 22 F.C.C.R. 6927, 7020 (Apr. 2, 2007) (further notice of proposed rulemaking).