cable

National Cable & Telecommunications Association
25 Massachusetts Avenue, NW, Suite 100
Washington, DC 20001-1431
(202) 222-2300

Michael K. Powell
President & Chief Executive Officer

(202) 222-2500
(202) 222-2514 Fax

August 22, 2011

Hon. Mary Bono Mack
104 Cannon House Office Building
Washington, DC 20515

Dear Congresswoman Bono Mack:

Thank you for your letter of July 18, 2011, requesting the National Cable & Telecommunications Association's ("NCTA") input concerning safeguards against the kind of "phone hacking" that was recently uncovered in the United Kingdom. NCTA shares your commitment to safeguarding American consumers against this practice, and we appreciate the opportunity to share the cable industry's perspective and expertise on this important issue. As discussed below, numerous laws and regulations already on the books in the United States minimize the threat of phone hacking and punish it if it occurs.

1. As communications through voice over internet protocol (VOIP), smartphones and other mobile devices become more integrated in our daily lives, do you expect to see a rise in phone hacking here in the United States (involving both personal conversations and voicemails) as criminals search for new ways to steal valuable information such as credit card numbers, bank accounts, Social Security numbers and biometric identifiers?

The proliferation of, and increased reliance on, new communications technologies and mobile devices can create new opportunities for hackers and other criminals. Network providers employ a variety of protective measures and technical safeguards aimed at deterring and detecting phone hacking. As with any criminal activity involving theft of personal property, however, there are some basic steps that individuals can take to mitigate the possibility of being victimized. These include securing their voicemail with a unique password, refraining from sharing that password, and changing it frequently.

2. At present, what safeguards do your member companies employ to ensure that American consumers are adequately protected against the type of phone hacking scandal currently being investigated in the United Kingdom?

NCTA's members have each developed and implemented a variety of technical measures and protocols to help ensure the security of their users' voicemail accounts. As a threshold matter, companies prevent or discourage the use of default or readily detectable passcodes, so that authorized users logging in to an account will identify themselves with a unique passcode.

Our companies have developed a range of protocols to protect against some of the most common strategies employed by hackers. For example, hackers generally cannot succeed unless they can convince the target network that they are legitimate authorized users by providing that unique

identifying information when prompted. In a "brute force" attack, the unauthorized party simply makes multiple attempts to guess the user's passcode. Some companies safeguard against brute force attacks by establishing complexity requirements for user passcodes in order to make guesswork more difficult. Many systems automatically cut-off account access after a pre-set number of incorrect login attempts unless and until the user's identity can be verified by other means.

In other instances, hackers may call telephone carriers impersonating the hacking victim (a technique sometimes referred to as "social engineering" or "pretexting") and obtain or reset the voicemail PIN code to acquire access to voicemail records. This practice is already addressed through the FCC's customer proprietary network information (CPNI) rules, which apply to all voice providers, including common carriers, wireless providers, and providers of interconnected VoIP service.[1/] Those rules prohibit voice providers from disclosing customer information without first taking steps to authenticate that the caller is actually the customer. They also require providers to notify customers immediately when a new password or other account authentication information is created or changed and to notify the FCC, law enforcement, and customers of any security breach.[2/] Providers must certify annually to the FCC that they are in compliance with the CPNI rules.[3/]

Many providers offer additional layers of protection that users can opt into. For example, although users typically do not need to enter a passcode when accessing voicemail from their own telephones or mobile devices, customers can opt to require passcode entry no matter where they are calling from. This is an effective weapon against "spoofing," in which an unauthorized party uses false caller-ID information to convince the system that the call is coming from the victim's own phone.

3. In the wake of this scandal, do your member companies believe it is necessary to adopt new practices to ensure that consumers in the United States are better protected in the future?

Although our members are continuously striving to develop new strategies to protect consumers, we are very confident in the safeguards currently offered.

1/ 47 C.F.R. Part 64, Subpart U.

2/ 47 C.F.R. §§ 64.2010, 64.2011.

3/ 47 C.F.R. §§ 64.2009(e).

4. Do you believe existing laws and regulations adequately protect consumers in the United States from phone hacking and similar privacy breaches?

Yes. In addition to the CPNI rules described above, existing laws provide powerful and effective tools for deterring and punishing the type of phone hacking activity alleged to have taken place in the United Kingdom.

The Electronic Communications Privacy Act ("ECPA") provides stiff criminal penalties for the types of hacking activities currently under scrutiny in the United Kingdom. Title I of ECPA prohibits not only the intentional interception of any wire, oral, or electronic communications, but also the disclosure or use of the contents of communications known to have been unlawfully intercepted. Violation of Title I can be punished by a fine and up to five years imprisonment.[4/]

Title II of ECPA, also known as the Stored Communications Act ("SCA"), creates an additional layer of protection for electronically stored communications, such voice-mail and e-mail.[5/] In addition to whatever penalties may apply under Title I of ECPA, violations of the SCA that are committed for commercial advantage, malicious destruction or damage, or private financial gain, may be punished by a further fine and up to five years for the first offense, and ten years for any additional offense.

The SCA also allows individual victims of this type of hacking to seek appropriate relief directly from the offending hacker in civil court.[6/] Under the statute, "appropriate relief" can include actual damages suffered by the victim, plus any profits that resulted from the violation, with a minimum recovery of $1,000. In some cases, the court may also assess punitive damages and reasonable litigation costs and attorneys fees, giving victims further incentive to seek relief and would-be hacker further discouragement.

The Telephone Records and Privacy Protection Act of 2006[7/] makes it a crime punishable by up to ten years imprisonment to knowingly and intentionally obtain (or attempt to obtain) or transfer confidential phone records information through fraud or misrepresentation or without authorization from the customer.

Section 705 of the Communications Act provides additional criminal liability for certain invasions of consumer privacy. That law prohibits the unauthorized publication or use of the contents of any communication made by wire or radio.[8/] When committed for the purpose of any commercial advantage or financial gain, violations of this provision may be punished by fines of up to $50,000 and two years imprisonment ($100,000 and five years imprisonment for repeat

---

4/ 18 U.S.C. § 2511.

5/ 18 U.S.C. § 2701.

6/ 18 U.S.C. § 2711.

7/ 18 U.S.C. §§ 1039(a), (b).

8/ 47 U.S.C. § 605.

offenders). Similar penalties can be incurred for the unauthorized interception of any communications service offered over a cable system.[9/] Both of these laws also permit victims to bring civil action against the offender.

Finally, the Truth in Caller ID Act[10/] specifically targets "spoofing," a common phone hacking practice of using false caller ID information in order to obtain access to voicemail. Violators of the Truth in Caller ID Act, which prohibits knowing transmission of misleading or inaccurate caller identification information "with the intent to defraud, cause harm, or wrongfully obtain anything of value," are subject to civil penalties or criminal fines of up $10,000 per violation.

In addition to these industry-specific deterrents, federal prosecutors can often add criminal charges of conspiracy[11/] and/or wire fraud[12/] to impose further liability and harsher penalties.

Federal law is not the only source of protection and deterrence against phone hacking. State criminal law also can provide additional tools to address such conduct, and individual victims also could seek to recover damages from hacking via common law tort claims against misappropriation of property.

5. Approximately how many phone hacking incidents are reported by your member companies in a year? Are the number of incidents growing or declining?

As of the present time, none of our member companies have received any reports of confirmed or suspected phone hacking incidents. It is worth noting that if a person gains unauthorized access to a customer's voicemail because that person has unlawfully obtained a customer's voicemail passcode or the customer has not changed his or her default passcode, the customer's voice provider may never be notified of the incident.

6. As a matter of practice, are phone hacking incidents, or suspected incidents, reported to law enforcement agencies and regulatory agencies?

Member companies are diligent in reporting relevant breaches of security to the FCC, law enforcement, and customers as required by regulation. Each member also expressed that it would cooperate fully with customers and law enforcement in the event of a known phone hacking incident.

9/ 47 U.S.C. § 553.

10/ 47 U.S.C. § 227(e).

11/ 18 U.S.C. § 371

12/ 18 U.S.C. § 1341

7. From a technological standpoint, how difficult is it to hack into cell phones or other mobile devices.

We rely on the equipment vendors to build in technological safeguards against hacking.

8. What steps can consumers take on their own to better protect their personally identifiable information when communicating through either fixed wire or wireless devices?

The most important step consumers can take to protect themselves against hacking is the selection of a unique and secure passcode that is never shared with anyone else. Users should never rely on default passcodes and should change their passcodes on a regular basis. Consumers should also take advantage of any and all optional safeguards offered by their service provider as well as those provided by their telephone or mobile device manufacturer. Customers can greatly reduce the risk of hacking by layering additional safeguards at every step of the log-in process. For example, a user who takes advantage of both a mobile device's "auto-lock" feature and a service provider's passcode requirement option is doubly protected from both spoofing and social engineering. These simple steps are already available to consumers and when used appropriately are extremely effective in safeguarding privacy.

Thank you again for the opportunity to share NCTA's perspective on this critical issue. I sincerely hope that the responses above help shed light on the current state of consumer privacy in our industry. Our member companies take their responsibilities toward consumer privacy very seriously, and NCTA is happy to provide your office with additional assistance as needed.

Sincerely,

Michael K. Powell
President & CEO
National Cable & Telecommunications Association