

Lessons from the NSA Warrantless Wiretapping Controversy

As most of you undoubtedly are aware, recent reports have alleged that the National Security Agency (“NSA”) carried out two comprehensive electronic surveillance programs with the aid of AT&T and several Bell Operating Companies. According to the reports, the NSA intercepted and analyzed millions of Americans’ telephone and Internet communications and obtained access to their Customer Proprietary Network Information (“CPNI”) without obtaining the necessary court orders or undertaking other legally required measures.

The recent media reports quickly were followed by several federal class action lawsuits seeking billions of dollars in damages from the carriers that allegedly cooperated with the NSA. The case that has advanced the furthest so far is *Hepting et al. v. AT&T*. That case deals with reports that the NSA engaged in “vacuum cleaner” surveillance of millions of international telephone calls and electronic messages. Plaintiffs in that matter represent individuals whose calls allegedly were tapped without appropriate legal authority, and they are pursuing damages under several theories.

Specifically, the plaintiffs argue that AT&T, acting as an instrument of the government, violated plaintiffs’ reasonable expectations of privacy and denied them the right to be free from unreasonable searches and seizures under the Fourth Amendment, and violated their First Amendment rights to speak and receive speech anonymously and associate privately. Plaintiffs also allege violations of the Foreign Intelligence

Surveillance Act (“FISA”) (governing access for foreign surveillance purposes), the Stored Communications Act (“SCA”) (governing access to “stored communications” including voicemail and email), the Pen Register statute (governing pen registers and trap and trace devices), the Electronic Communications Privacy Act of 1986 (“ECPA”) (governing real time access to oral and electronic communications), and Sections 222 and 605 of the Communication Act of 1934 (governing the use of CPNI, and governing disclosure of interstate or foreign communication without authorization, respectively). The Department of Justice has moved to intervene and asked that the case be dismissed under the state-secrets privilege.

Additionally, the American Civil Liberties Union has filed complaints in 21 states alleging that AT&T and Verizon violated state laws concerning the disclosure of CPNI. The ACLU also sent a letter to the FCC urging it to reconsider its refusal to investigate reports that AT&T, Verizon and BellSouth allegedly cooperated with the NSA to enable the government to spy on millions of Americans.

The government surveillance programs and the resulting litigation highlight the need for carriers to strengthen their policies and procedures for providing the government with access to their networks and disclosing CPNI. Accordingly, we recommend that carriers take the following steps to better protect themselves from potential liability:

1. Review your procedures for providing access to law enforcement agencies. Law enforcement can request information under various laws, each of which provides different procedures for accessing information. The principal statutes are the ECPA, the SCA, the Pen Register statute and FISA. Notably, each of these statutes permits warrantless searches in limited circumstances. In addition, the President has statutory powers over communications networks during a state of war and in case of the “threat of war,” as well as certain asserted Constitutional powers to engage in the national defense. Telecommunications carriers should review these statutes carefully to ensure that internal procedures for handling law enforcement requests comply with these procedural and substantive standards.

2. Incorporate your procedures into your CALEA Manual and into your CPNI Policies. In addition to compliance with the principal federal wiretapping statutes outlined above, carriers must also comply with federal rules implementing those statutes. For example, the FCC’s rules implementing CALEA require carriers to file a CALEA compliance manual with the FCC. Additionally, the Commission recently extended its CALEA requirements to facilities-based broadband Internet access and VoIP providers (see http://www.kelleydrye.com/resource_center/client_advisories/0125 for Kelley Drye’s Client Advisory). To the extent that you have already filed a CALEA com-

pliance manual with the FCC, you may need to revise the manual and re-file it to reflect changes to your company’s policies or procedures resulting from changes of law or as otherwise necessary. Similarly, FCC rules require each telecommunications carrier to conduct an annual review of its CPNI policies and to have an officer certify that the policies comply with Section 222 and FCC rules. We recommend that carriers incorporate their procedures for disclosing customer information to law enforcement into its CPNI policy/officer certification.

3. Consider revising your CPNI disclosures to consumers to address your procedures in more detail. Many carriers currently use a disclosure that says the company will not disclose CPNI except “as required by law,” mirroring the statutory language in Section 222. The NSA cases demonstrate that these disclosures may themselves be inadequate, for the legal obligation to disclose CPNI and the circumstances under which it is appropriate to do so are not as simple as conveyed in the typical CPNI disclosure. To avoid claims alleging a failure to adequately explain the company’s procedures, we recommend that you consider disclosing the circumstances under which the company provides assistance with law enforcement information requests.

We will continue to follow the NSA cases as they develop. If you would like further updates, please contact us.

**For more information
please contact:**

Steven Augustino
(202) 342-8612
saugustino@kelleydrye.com