Privacy Protection Under the Communications Act

Remarks of FCC Commissioner Kathleen Q. Abernathy
Federalist Society Conference
Washington, DC -- November 14, 2002
As Prepared for Delivery

Thank you, Judge Williams. I have to admit, I'm a little nervous about having Judge Williams moderate this panel discussion – I'm concerned that if I get anything wrong, it will be vacated and remanded. . . . But I'll do my best not to misconstrue the Communications Act or the FCC's rules, and, with any luck, I'll get a little *Chevron* deference.

I thought I would talk today about privacy issues that arise at the FCC. This is actually a rather small universe because there are only two statutes that we enforce relating to privacy – but our statutory universe, though small, is a very interesting one because it intersects with constitutional law in some unexpected and perhaps even counterintuitive ways.

First, the two statutes.

The first, section 222 of the Communications Act, regulates customer privacy interests in their information held by telecom carriers – known as customer proprietary network information, or CPNI. This includes information regarding calling patterns and usage of various features such as voice mail or caller ID. The statute regulates this private-private relationship – between customer and the telecom provider – by protecting the customer from having his information misused by the telecomm provider. Primarily, it aims to protect customer privacy by restricting the marketing practices of telecom carriers.

The second statute, the Communications Assistance for Law Enforcement Act (or CALEA for short) aims to require telecom providers to make their networks capable of being used by law enforcement officers seeking information about telecom users. This statute therefore regulates the government-private relationship – the interaction between government prosecutors or police and private citizens. And, of course, it's different from the first statute because it actually appears to *diminish* privacy in some respects by making information that might otherwise be private into more easily identifiable and snoopable information. (In effect it requires telecom companies, when implementing new technologies to make those technologies compatible with electronic surveillance by law enforcement.)

While there are many details I won't be able to cover today, the key point I want to leave you with is that, in implementing each statute, the FCC has sought to balance the substantial governmental interest in protecting privacy against countervailing statutory and constitutional interests. The courts have played a role in helping strike this balance. Here is the preview of the story: in the section 222 context, the courts have helped us see that countervailing constitutional interests actually limit Congress' attempts to protect privacy; in the CALEA context, the courts have helped us see that countervailing constitutional interests limit the government's ability to intrude onto privacy interests.

Section 222

A newcomer to this area of law might guess that the protection of consumer information under section 222 would be stronger than the privacy protections afforded under CALEA: the consumer information looks intuitively private and the telecom carrier's interests in using the information appear to be merely commercial. Indeed, the FCC initially took such a view.

But the Constitution is a major complicating factor that makes the outcomes somewhat counterintuitive. As the Tenth Circuit has made clear, telecom carriers have a substantial First Amendment interest in using "customer proprietary network information" – customer service info -- to communicate with their customers. In other words, the telecomm companies have their own rights – *constitutional rights.* And looking at section 222 from the consumer's perspective, they have no *constitutional* protection of their own from invasions of privacy by telecom carriers, because the telecom carriers are not state actors.

I'll now turn to how the FCC has responded to this interplay – how we have interpreted section 222 and the court decisions that have required adjustments to the implementing regulations.

Section 222(c) defines CPNI as information that is made available by virtue of the customer-carrier relationship and that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service. Practically speaking, this typically means information regarding the phone numbers a customer calls, the duration of calls and other information that reveals calling patterns, and the services and features that a customer purchases. Subject to a few exceptions, the Act states that carriers may not use or disclose this info without a customer's "approval."

When the FCC first implemented Section 222, in 1998, it construed the term "approval" strictly and therefore required carriers to obtain *express* consent for the use or disclosure of CPNI outside the context of the existing service relationship. For example, a carrier could use the info to market a feature such as caller ID to an existing local customer without first getting specific permission, but it could not use the info to market other telecommunications services, such as wireless or long distance. This form of approval is generally known as "opt in" approval.

On appeal, the Tenth Circuit noted the First Amendment interest of the telecom carrier in communicating with its customers. With this First Amendment interest in mind, the court examined the FCC's rules under heightened scrutiny. It vacated the "opt in" requirement as inconsistent with the First Amendment and remanded the order for further consideration. According to the court, the FCC flunked the narrow tailoring requirement because it did not adequately consider an "opt out" approval scheme – that is, a requirement that carriers notify customers of their intention to use CPNI and give the customer an opportunity to contact the carrier to deny consent. This approach puts the onus of protecting privacy on customers, rather than on carriers, consistent with other precedents permitting speakers to make contact unless and until a listener states that he is not interested in receiving communications.

On remand, the Commission adopted an order in July that took a bifurcated approach. When it comes to the disclosure of information by a carrier to an unrelated third party -- which is a situation where the consumer's expectation of privacy is greatest and the carrier's First Amendment interest in speaking to the customer is weakest -- the Commission reinstated an opt-in requirement. Where a carrier seeks to use customer Info

in marketing its *own* services to the consumer (or those of a joint venture partner to the consumer), the consumer has a lesser expectation of privacy because of the existing business relationship, and the carrier has a much stronger First Amendment interest because of its interest in speaking to its own customers. The Commission accordingly adopted an opt-out approach for such situations. I was pleased to support this bifurcated approach, because I believe it is narrowly tailored to the privacy interests at stake. But there is no doubt that this approach overall is less protective of privacy than the Commission's initial order; and that is a direct and inevitable consequence of the need to balance the First Amendment rights of the carriers against consumer privacy expectations.

CALEA

The FCC's implementation of CALEA also has been up to the court of appeals and back, although in this case the remand order is more consistent with the original approach.

Recall that CALEA, in section 103, requires carriers to ensure that their equipment and services are capable of isolating and allowing the government to intercept communications as well as call-identifying information. Call-identifying information is defined as dialing or signaling information that identifies the origin, direction, destination, or termination of a communication. This includes not only the telephone number dialed at the outset of a call, but also numbers dialed during a call and any tones or notifications, such as a busy signal. Although the statute works to diminish privacy by making information more readily accessible, it also directs carriers, in meeting the government's needs, to do so in a manner that protects the privacy and security of information that is *not* authorized to be intercepted.

Much of the controversy surrounding the implementation of CALEA relates to the means of identifying so-called "call-identifying" information (as opposed to any other information). An industry group developed standards for various electronic surveillance capabilities, and the Department of Justice and FBI developed a punch list of additional desired capabilities. The government and industry were able to agree on several punch list items, but several groups ultimately filed a petition for review challenging four requirements. While the D.C. Circuit upheld parts of the FCC's order, it vacated and remanded that part of the Commission's decision that required implementation of the four disputed punch list items.

I won't bore you with a discussion of the particulars of the disputed capabilities; suffice it to say that this is a very complicated subject. What is important for our discussion today is that the appeal focused on whether the FCC met the standard for imposing technical requirements *over* the industry's objection. The court held that the FCC did not adequately explain why the capabilities at issue would in fact identify call-identifying information, as opposed to the content of a call. The Commission also failed to explain why the capabilities were cost-effective and would adequately protect the privacy and security of citizens' communications not authorized to be intercepted. In other words, the Court of Appeals in part required the FCC to respect the constitutional privacy rights of individuals from government intrusion.

The Commission released its order on this issue on remand last April and reinstated the requirement to implement the four punch-list capabilities at issue. We held

that each capability identifies call-identifying information, is cost-effective, and sufficiently protects privacy. With respect to the privacy issue, the Commission focused on the fact that law enforcement agencies must seek and obtain from an appropriate court the necessary authorization to conduct surveillance operations – thus interpreting the Fourth Amendment as expressly authorizing, under proper circumstances with a warrant, a limited intrusion onto what otherwise would be legitimate privacy interests. Let me give an example: In authorizing a particular legal instrument – such as a pen register order – the court must determine the sort of information that the carrier must turn over. If the court authorizes a pen register and also authorizes what is known as dialed digit extraction, the carrier must have that capability. But if the court does *not* authorize dialed digit extraction, then the carrier must turn off that capability. This court oversight process, together with the carrier's ability to turn surveillance capabilities on and off, are key factors in protecting the privacy of information that is not authorized to be intercepted.

I'll stop at this point, because it would use the entire hour and a half we have set aside just to describe the various punch list items required under CALEA. But in closing, let me re-emphasize my principal point: despite the various differences between section 222 and CALEA, the FCC's goal in implementing each statute has been to thread its way between and accommodate competing privacy concerns, some found in statute and some in the Constitution. I hope we have been successful in that effort, and I look forward to hearing from the other panelists about how we can do better.