

## EDITORIAL

## What the Synnex case means

A closely watched New Jersey appellate case arising from a multi-million dollar burglary could dramatically impact the ability of alarm companies in New Jersey, and possibly elsewhere, to limit claims by subscribers. In the case, *Synnex v. ADT*, a New Jersey trial judge refused to enforce the alarm company's contract terms limiting its liability to its subscribers, holding that the state's alarm licensing statute rendered the clauses un-

enforceable. Following trial, the jury

found the alarm company negligent and awarded the subscriber's insurer more than \$4 million.

ADT appealed the decision and the New Jersey appeals court scheduled oral argument for May 1.

The facts of the *Synnex* case are complicated. Here's a thumbnail sketch from my review of some of the appellate briefs filed by the parties:

Synnex, a multi-billion dollar information technology provider, contracted with ADT to provide security at a new warehouse in Edison, N.J., where Synnex stored equipment. ADT serviced a system at another Synnex warehouse

in New Jersey. Synnex wanted ADT to install a system at the new warehouse and to incorporate the radio back-up from the existing system at its other warehouse. Synnex also wanted the new system to include cellular back-up.

ADT installed the new system but the existing radio backup was incompatible and ultimately, never incorporated.

Nine months after Synnex signed the ADT contract, burglars entered the Edison facility, tripping detectors that transmitted

signals to ADT's central station.

The burglars cut the telephone

lines and destroyed the cellular back-up, effectively disabling the system. According to Synnex, ADT alerted police and then contacted a Synnex employee, telling him that he did not need to go to the facility unless ADT heard back from police. The burglars made off with more than \$7 million in equipment from the facility.

Synnex's insurers covered the company's loss and then instituted a lawsuit against ADT. Synnex claimed that radio back-up would have enabled the system to transmit signals even if the telephone lines and cellular back-up had been breached. In addition, Synnex claimed, a radio back-

up would have enabled ADT to confirm that the system remained operational during an attempted burglary.

Synnex also contended that ADT was aware burglars exploited systems that relied solely on cellular back-up in exactly the way that the burglars had at the Edison warehouse: breaking in to trigger the alarm, cutting the telephone line, destroying the cellular back-up, hiding until police left, then re-entering the premises unimpeded.

Before the case went to trial, ADT asked the court to enforce the indemnity and exculpatory clauses in its contract. ADT argued that Synnex should indemnify ADT against the claims of its insurer and that ADT's liability was limited by the express terms of the contract. The trial court, however, refused to enforce the agreement because ADT's contract required written approval by ADT's authorized representative, who failed to sign the contract. Although the parties executed riders for additional services and equipment, which expressly affirmed the terms of the original contract and which were signed by Synnex and ADT's authorized representative, the court refused to enforce the contract.

The trial court also held that, even if the ADT contract were enforceable, the limitation of li-

ability provisions in the contract were not legal under the state's 1998 alarm licensing law. (Before 1998, New Jersey courts enforced similar clauses in alarm contracts limiting the liability of alarm companies for negligence.)

The trial judge placed significant importance on a recent appeals court decision holding that home inspectors, licensed under a state law passed on the same day as the alarm licensing law, were deemed to be "professionals" under the new state law and, therefore, could not legally limit their liability. The trial judge reasoned that alarm contractors, licensed under the "Alarm Professionals Law," likewise could not limit their liability.

There are dramatic differences between a residential home inspection, where a homeowner cannot insure against a botched home inspection, and a commercial alarm subscriber that can and should obtain insurance to protect against loss. There is also a big difference between consumer transactions and transactions between sophisticated, multi-national companies. But what was most surprising about the judge's decision was that he ignored well-settled New Jersey case law

enforcing limitation of liability provisions in security contracts. The trial judge also missed the fact that ADT's monthly monitoring fee was grossly disproportionate to the potential liability it would be undertaking without their contractual limitations clauses. Courts in other states, most notably New York, have recognized this principal in cases that have focused on keeping security services affordable.

Based on my review of the briefs, there are several valid grounds on which the appeals court can overturn the trial court's decision. I suspect there will be a reversal on at least one of these grounds. If not, the allocation of risk among alarm companies and subscribers will change dramatically in New Jersey and could signal the beginning of a trend in other states. If so, only the largest and most financially sound providers are likely to survive in the long term.

*Eric Pritchard is a lawyer at Kleinbard Bell & Brecker LLP in Philadelphia where he chairs the firm's electronic security practice. He can be reached at epritchard@kleinbard.com. Pritchard did not participate in the Synnex v. ADT litigation.*

## GUEST COMMENTARY



Eric Pritchard

## Be a nosy neighbor

*Continued from previous page*

The more complex the system, the more important it will be to have real-time access to a wireless network expert with the right tools and training for the job. For example, mesh networks, while powerful and flexible can be more of a challenge to maintain than simple hub-and-spoke multipoint or point-to-point backhaul systems.

Finally, include in the project budget a few spares of critical components to have on hand in the event of an outage. Be sure to also include items such as lightning arrestors, cabling and connectors that might become damaged during storms or power surges.

**Defending the RF spectrum at your location** As discussed in Part I, in the United States the FCC

is the regulatory body responsible for managing unlicensed spectrum (ISM bands). The hard truth is that if your neighbor has installed an FCC-approved radio transceiver that is transmitting RF energy into your property and interfering with your wireless devices, there is very little recourse available to you. However, if they have installed *illegal* power amplifiers, and you can measure and document this overpowered signal, you do have the right to file a petition with the FCC to have these disconnected and the offender fined.

**Protecting your investment/future-proofing your network** The most sophisticated wireless network designers today very carefully manage the unlicensed spectrum in their domain. Because of the rapid growth in the

introduction of new Ethernet based products, they realize that at any time they may be called upon to add new network products while maintaining the current systems already in place.

For example, installing a high-powered frequency-hopping product can consume the entire ISM band at your property; thereby preventing you from installing a new wireless product down the road. Manage your spectrum wisely now, and you will be able to install next-generation products without rendering your current investment obsolete.

**New wireless networking technologies, but will these help?** In the past several years, tremendous advances have been made in the field of wireless wide area networking. For example, WiMAX and 4G cellular networks will provide homes, businesses and mobile users with a broadband alternative to the

current DSL and Cable offerings. However, these technologies are in licensed bands, have limited upload speeds, required monthly subscriptions, and so are not easily applicable to the requirements of wireless security devices. Therefore, it appears that for the foreseeable future most wireless security and surveillance products are very likely to be limited to the unlicensed ISM bands.

Shannon's Theorem defines the maximal amount of data that can be carried by a given RF channel. For example, a 1MHz-wide slice of spectrum (say between 900-901 MHz) can be modulated to transmit approximately 800,000 bits of data per second. This is

the current state of the art, and in order to improve upon this, design engineers will have to devise new technologies not yet conceived to squeeze more data through a fixed amount of spectrum.

Until this happens, our unlicensed ISM bands will become increasingly crowded. Therefore, like any finite resource on our planet, we must all be disciplined and only design and implement systems that are efficient in their use of this limited spectrum and hence play well with others.

*Ray Shilling is the vice president of sales and marketing at AvalAN Wireless. He can be reached at rshilling@avalanwireless.com.*

## CORRECTION

In our Central Station sourcebook, published in February, we printed some incorrect information. Alarm Central LLC can be contacted at 877-532-1500, has a range of monthly monitoring fees from \$4 to \$6, and should have been listed as being 5-Diamond certified, with UUFEX, billing services, a dealer program, and financing options. The Security Center can be contacted at 800-437-4635.

Also in our February issue, in the story "UL SQ 561 Confuses in Canada," David Currie was mistakenly identified as David Curry.