MINNESOTA LAWYER

May 8, 2009 12:18 PM CDT

'Spoofing' caller ID systems create evidentiary hang-ups in some cases

by Barbara L. Jones Associate Editor

Minneapolis attorney Kristine Zajac helped a client secure a dismissal by presenting evidence that caller ID can be fooled by spoofers. (Photo: Bill Klotz)

Caller ID is a great modern convenience, allowing people to avoid calls from telemarketers, ex-spouses and other undesirables. We see a name or number on the screen and believe it accurately states who is on the other end of the line. But it doesn't always.

There is an increasingly common and completely legal practice called "spoofing" that allows a caller to manipulate what number shows up on a caller ID screen as the source of the phone call. And there's an abundance of information on the Web saying how to do it. "SpoofCard — be who you want to be," advertises one site. For $10 for 60 minutes, the purchaser gets a personal identification number and then dials a toll-free number. The individual is then prompted to enter the destination number and the number that person wants to appear on the caller ID screen at the call destination.

Spoofing can also be accomplished using voice over Internet protocol or other Internet/telephone communications practices.

So given that the practice is legal, what does spoofing have to do with lawyers?

Evidence of the practice of spoofing recently convinced Hennepin County District Court Judge Janet Poston to find for a defendant charged with violating his probation. The state alleged the man had contravened a no-contact order by texting a message to his ex-wife.

The message was sent to the ex-wife's landline; she heard it as a digital voice using audio technology. The defendant's cell phone number was displayed on the caller ID box. The ex-wife contacted law enforcement because the defendant was on probation for a gross misdemeanor harassment charge and ordered not to contact her. Based on the alleged contact, police arrested the man.

The man's lawyer, Kristine Zajac of Minneapolis, presented expert testimony at the defendant's probation revocation hearing that the message could have come from a spoofer using the defendant's number.

"I testified that a caller ID number is similar to a return address on an envelope," said mobile communications and computer forensics expert Jeff Wold.

All records had been erased from the defendant's cell phone, and the phone records from the telephone company had not been subpoenaed. Accordingly, Wold testified that the evidence that the defendant had placed the call was inconclusive. "Caller ID is not an acceptable way to show who placed a call," Wold said.

The judge agreed. Finding that the state had not met its burden of showing that the message had in fact come from the defendant, she declined to revoke probation.

Businesses do it

Businesses spoof all the time, according to Wold. Businesses do it to hide the direct dial number of a person at a company, and debt collectors and telemarketers have obvious reasons for concealing their phone numbers.

While spoofing cards are available for purchase, the components to build the equipment to spoof via computer are readily available, as is the necessary software, Wold said. "The phone system is just a computer. Parts are widely available."

E-mail can also be spoofed, Wold said. Wold told Minnesota Lawyer that he testified in a custody case in which a mother used information about the father to create e-mail accounts in his name and then sent herself intimidating messages to influence his custody chances. Wold was able to establish that the e-mails had originated from the mother's ISP at a time when the father was not present in the geographical area.

"You could go through calisthenics to send an e-mail (from another location), but it wasn't reasonable to think the father had done it," Wold said.

While spoofing has been common for quite some time, there is a dearth of caselaw on its use. However, the practice has made it into the popular culture. An instance of spoofing was integral to the plot of a recent episode of NBC's "Law and Order: SVU."

Hamline University S chool of Law Professor Peter Thompson, who teaches evidence and criminal law, said he is unaware of any case in which spoofing has been raised. Although Rule 901 (b) (6) discusses the authentication of telephone conversations, it does not directly address caller ID questions, he said.

The foundation for the information on the caller ID box should be laid, Thompson advised. "If the box were the only evidence, I'm not sure I'd send [the case] to the jury," he added.

Spoofing's days numbered?

While spoofing itself is not a crime, using it to further a criminal enterprise is. In 2008, evidence emerged of a conspiracy of “phone phreaks” who hacked into telephone company equipment to report emergency calls, caus ing SWAT teams to respond to people’s homes. The three lead defendants were each sentenced to 60 months in prison plus payment of restitution. In other cases, telemarketers have been fined for using spoofing to evade Do Not Call list prohibitions.

There is currently federal spoofing legislation in the pipeline. The Truth in Caller ID Act, an amendment to the Communications Act of 1934, would prohibit manipulation of caller ID information with the intent to defraud, cause harm or wrongfully obtain anything of value. The law would except law enforcement agencies and actions pursuant to a court order.

The bill, which is co-sponsored by Minnesota Senator Amy Klobuchar, is pending at the Committee on Commerce, Science and Transportation. Similar legislation is before the House Committee on Energy and Commerce.