Online Ethics Center
FOR ENGINEERING AND SCIENCE

LaMacchia Case Raises Legal Questions of Fraud

Author(s)

Jeremy Hylton

Year

1994

Description

Second of a two part article about the legal implications of this trial and the free speech issues that arise when prosecuting a crime of this nature.

Body

Last Friday morning, David M. LaMacchia '95 pleaded not guilty to one charge of conspiracy to commit wire fraud in the Boston federal district court.

Much of the discussion of the case, both in the media and on Usenet, has focused on whether software piracy is right or wrong, and how the government would prove that LaMacchia was involved in pirating software. But lawyers familiar with the case are quick to point out that software piracy is not at issue.

The case will have important implications for "how the principles underlying freedom of speech and of the press will be applied to the world of communications," wrote Harvey A. Silverglate, a lawyer for LaMacchia.

While so much discussion has focused on the legal implications of the case, Professor of Computer Science and Engineering Harold Abelson PhD '73 is concerned that people at the Institute have forgotten about the student at the center of the case.

"They've forgotten that he's a real person. He's a real, 20-year-old MIT junior who's in the middle of a legal test case, and he's facing terrifyingly serious consequences," Abelson said.

If convicted, LaMacchia could face penalties up to 5 years in prison and $250,000 in fines.

"I'm really upset at some of the flaming I've been hearing around campus: comments that are extremely stark and also self-righteous," Abelson continued. "I wish that the people who are arguing so self-righteously would remember [the consequences LaMacchia faces] and show a little compassion and tact."

The outcome of LaMacchia's case will depend, in part, upon the prosecution's ability to make the wire fraud law, written in 1952 to apply to telephone lines, apply to a case involving computer networks.

The charge that was entered against LaMacchia suggests that the government had trouble finding a specific law that applied to the case, according to Mike Godwin, staff counsel to the Electronic Frontier Foundation. "If you look at the underlying crime, it's not very easy to figure out how his alleged conduct relates to any of them," Godwin said.

"I think the government believes that it would be very hard to prove he was doing it for profit," Godwin said. Instead, the government is using a "general purpose statute [that it turns to] whenever the more specific statutes don't seem to fit - and one of them is wire fraud."

"It's relatively easy to make the wire fraud statutes fit the crime," Godwin continued.

Instead of proving that copyright violations were committed, the government will need to prove two things to win a conviction of the conspiracy charge, Godwin said. First, the government must show that LaMacchia worked with at least one other person to commit a crime. Second, the government must show that the crime, which the conspirators intended to commit, meets all the standards for a wire fraud

charge.

In a conspiracy case, the prosecution must prove that two or more people agreed to a plan to commit a crime. It must also prove that at least one person took actions towards carrying out that plan.

The prosecution must also show that the intended actions of the conspirators exactly match standards for the crime the defendants are charged with conspiring to commit.

"If it's conspiracy to counterfeit, you have to map out all the elements of the underlying crime," Godwin said.

Proving the connection to the underlying crime may be difficult in this case, Godwin said. "Although the [wire fraud] statute is pretty broad, it's not so broad that it includes the defendant's alleged conduct," he said.

"Normally in other kinds of fraud crimes, there's some deception. Where's the fraud? Who did he lie to?" Godwin asked.

To commit a fraud, a person must misrepresent him or herself to another person. That misrepresentation must be to the detriment of the other person and the person committing the fraud must gain something of value, Godwin explained.

The indictment prints several files titled Readme that were placed on the site that LaMacchia ran; it charges that LaMacchia placed them using the aliases "John Gaunt" and "Grimjack."

One file listed SimCity 2000, Excel 5.0, and WordPerfect 6.0 and said, "If anyone has this stuff, I'd appreciate it." Another warned users that if the existence of the distribution site became known it could be "purged" by the "net cops."

Godwin questioned how important the messages were to the case. "I'm not sure they are significant at all." The messages do not prove that LaMacchia deceived the service's users or that he profited from the distribution of the software, he said.

Free speech issues raised

In a defense primer circulated earlier this week, Harvey A. Silverglate, LaMacchia's lawyer, outlined how the case could affect future cases involving computer communications and freedom of speech.

Silverglate said the case has serious implications for people who operate computer bulletin boards. Godwin agreed with that characterization of the case.

"It's very clear that Scaron; what they're trying to do is to create a conspiracy to make him liable for everyone who used that [File Service Protocol] site," Godwin said.

Silverglate questioned whether system operators should be held responsible for everything that users do while logged onto their systems. The Constitution "has long conferred special protection on those engaged in the activity of maintaining communications media," Silverglate said.

Godwin suggested the analogy of prosecuting the *Boston Phoenix* because some of its adult services advertisements were really fronts for prostitution. "The *Phoenix* has ads for escort services and massage parlors that the editors clearly know are fronts for illegal activities. You'd have to be stupid not to, but no one says that the *Phoenix* is aiding and abetting," he said.

The question is whether First Amendment protections "should apply fully to those in the print medium," Silverglate said. "Because the law has been slow in adjusting to the age of digital communications, there have been relatively few legal tests of the scope of First Amendment protections in cyberspace."

Though the law's slow pace in adjusting to changes in technology can be frustrating, Professor Randall Davis, associate director of the Artificial Intelligence Laboratory, cautions that the slow pace may be just what is needed.

"There's a long-term perspective that is particularly important, even though it's frustrating when dealing with a fast-moving technology. We should give that long-term perspective its due because people will likely have to live with the laws for a long time," Davis said.

Notes

Author: Jeremy Hylton, Chairman.

Rights

Use of Materials on the OEC

Resource Type

Case Study / Scenario

Topics

Security
Privacy and Surveillance

Discipline(s)

Computer Sciences
Computer, Math, and Physical Sciences

Publisher

Online Ethics Center