Typhoid Mary

"I bet you wouldn't have done anything about this case, and you'd have been wrong," said Kim's counterpart from another university, as the two were waiting to get a T-shirt from a vendor's booth at a conference.

A student's dormitory-room computer on our campus had a directory that was entirely open to anyone writing or reading files using standard Internet protocols - a drop box, in network parlance. A "readme" file in the directory suggested that people put files or programs into the open directory for others to download. In the directory we found source code for virtually every known DOS virus, which was therefore available to everyone on the Internet.

Kim's colleague knew that Kim's University for the most part neither monitored nor censored the materials students and other network users made available on or downloaded from the Internet. There were three major exceptions: publishing or copying that violated Federal or State law (such as unlicensed software distribution), uses that threatened system integrity or functionality (such as chain letters or badly-designed network games), and postings or other communications that violated the University's rules about harassment and other uncivil behavior. Kim's colleague thought these exceptions were too narrow, and had long tried to persuade Kim that Another University's policies and procedures made more sense.

We shut this jerk's network connection off (Kim's colleague continued), *and obtained a cease-and-desist order from the campus Judicial Officer. The connection is going to stay off until the disciplinary process renders a judgment.*

"Would we really have let this student keep operating?," Kim said later to the academic-computing staff. "Not that anyone at our University would do such a thing - that's the kind of thing Another University students do, not ours - but what shall we do if it happens? Should we be doing anything to prevent it?"