11-13-1998

Taking a Byte Out of Cybercrime, Law Students Drafting Computer Crimes Code

Follow this and additional works at: https://ecommons.udayton.edu/news_rls

Recommended Citation
https://ecommons.udayton.edu/news_rls/8641

This News Article is brought to you for free and open access by the Marketing and Communications at eCommons. It has been accepted for inclusion in News Releases by an authorized administrator of eCommons. For more information, please contact frice1@udayton.edu, mschlangen1@udayton.edu.
TAKING A BYTE OUT OF CYBERCRIME, LAW STUDENTS DRAFTING COMPUTER CRIMES CODE

DAYTON, Ohio — This was more than just cybermischief, a joy ride on the Internet. It bordered on the personal.

As University of Dayton law students mused online about how to deal with cybercriminals, hackers tapped into the public area of their password-protected site. One hacker later e-mailed professor Susan Brenner to complain that computer hacking is not a crime.

With the help of more than a dozen “virtual faculty” around the country — federal prosecutors, computer crime investigators, even an FBI agent — students in a new online cybercrimes seminar are drafting a model state computer crimes code to deal with digital abuse, such as computer hacking.

“My initial thought on being discovered by our ‘target audience’ is, well, ‘cool,’” said Geordie Garratt, a member of the class. Other students weren’t nearly as thrilled.

“I do get an eerie feeling just knowing that these hackers are watching us,” conceded classmate Hazel Rountree in a posting in the class discussion area. “I wonder if they’re able to break into our bulletin postings? What if they take ‘techno revenge’ on us and deliberately destroy our work in a manner that cannot be repaired? It just motivates me to make our model code as effective and as far-reaching as possible to protect innocent people,” she said. “Now that we have the potential of being victimized ourselves, this whole issue of cybercrimes is a reality.”

Elsewhere on campus, professor Brenner sat behind her computer and grinned at the exchange. For her students, this is not a simulated classroom exercise, or a page out of a science-fiction novel. It’s a strong dose of 21st-century legal reality, a brush with the dark side of cyberspace. With the click of a mouse, computer-literate criminals can rob banks, change hospital records, tamper with IRS records, sell alcohol to minors, embezzle, stalk others, damage a person’s credit rating — even impersonate a law enforcement officer (or anyone else).

Brenner, a former white-collar criminal defense attorney, worked with law student Brett Burney over the summer to produce www.cybercrimes.net — a Web site envisioned as a national clearinghouse on cybercrimes. Her colleague Rebecca Cochran, faculty adviser to the school’s moot court board, is organizing the nation’s first annual cybercrimes moot court competition, to be held on campus March 19-20, for law school teams around the country.
two law professors are helping a new generation of attorneys develop new laws for such intriguing-sounding crimes as cracking, hacking and phreaking.

Haven't heard of phreaking? It's the ability to control telephone lines, like the infamous Dark Dante, a.k.a. Kevin Lee Poulsen. “At the age of 12, Dark Dante could pick up a phone and whistle a perfect pitch — and bounce around the world for free,” said Brenner, marveling at the audacity of this new breed of criminals. “When he got older, he got control of a radio station’s telephone lines and won a Porsche as part of a contest. Ultimately, he was caught, arrested and prosecuted on mail and wire fraud, but it just shows the incredible power that one person can have. The Internet can put that kind of power in anyone’s hands. Twenty years ago nobody could have done that.

"Today, there’s even the potential for cybermurder,” she said. “A computer hacker could get into a General Motors’ computer and change the design of brakes, and people could die. Or someone could screw up the traffic lights in the city or shut down a water plant.”

The implications? “It’s becoming a field day for lawyers, but a nightmare for law enforcement officers,” Cochran said. “Cybercrimes are a growth industry.”

Though it’s difficult to pin down the cost of cybercrimes, a recent study by the American Society for Industrial Security estimates U.S.-based companies lose $250 billion worth of intellectual property each year. That doesn’t touch on other illegal activities committed with a computer, such as selling drugs or luring children.

That’s why UD law students are drawing upon the expertise of law enforcement officers and lawyers in the field to develop legislation they hope will eventually be adopted by states struggling with how to deal with computer crimes. While states have some laws on the books, no state has a one-size-fits-all code to deal with the gamut of emerging computer crimes, from information theft — dubbed “infojacking” — to invasion of privacy. Brenner plans to invite state legislators, law enforcement officers and lawyers to critique the draft code, and a class next fall will refine it.

“The students are amazingly knowledgeable about these areas of the law. It blows me away,” said Randy Alden, assistant federal public defender for the Southern District of Ohio, who has found himself tapping out his thoughts to students’ queries in the early hours of the morning, long after his 13-month-old baby is tucked in. “This kind of seminar allows students to get their hands on real-world issues that practitioners are grappling with. There’s a level of dialogue here that I didn’t get in law school.”

-30-

For media interviews, contact Susan Brenner at (937) 229-2929 or brenner@udayton.edu; Rebecca Cochran at (937) 229-2332 or cochran@odo.law.udayton.edu; Randy Alden at (937) 225-7687; and Hazel Rountree at rountrhd@flyernet.udayton.edu