Access Warrants, Plain Sight Regs -- UD Law Students Compile Model Code to Help Police Combat Cybercrimes

University of Dayton

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

Recommended Citation
https://ecommons.udayton.edu/news_rls/10489

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.
ACCESS WARRANTS, PLAIN SIGHT REGS — UD LAW STUDENTS COMPILE MODEL CODE TO HELP POLICE COMBAT CYBERCRIMES

DAYTON, Ohio — Thanks to law students at the University of Dayton, “access warrants” may become a common tool for law enforcement officials combating cybercrime.

The students also suggest privilege exists between an Internet service provider and its clients, meaning e-mail content is private and cannot be revealed by the ISP, and a list of computer files “in plain sight” on the screen doesn’t mean that content of the files is in plain sight and open to indiscriminate search.

A group of 28 third-year students at the University of Dayton School of Law has taken the lead in suggesting how police and prosecutors can best function in a world where the latest technology often outstrips conventional law enforcement practices. The students participated in Cybercrimes Seminar 2000, an online class taught by Susan Brenner, associate dean for academic affairs at the School of Law at UD, and their semester’s project was to develop a model code for investigating cybercrimes.

“This is so far ahead of the curve,” said Brenner, who connected her students with more than 30 experts ranging from a “white-hat” hacker to forensic investigators from the U.S. Department of Justice and New Scotland Yard. “Nobody else has the liberty of thinking about cybercrime as a whole. Judges and attorneys deal with pieces of it as certain cases come up, but we’ve had the opportunity to parse out all the issues that come up.”

According to an August 2000 brief from the U.S. Department of Justice, the Federal Bureau of Investigation estimates electronic crimes cost about $10 billion a year with only 17 percent of the companies victimized reporting the losses to law enforcement agencies. A 1999 survey conducted by the Computer Security Institute and the FBI of 521 financial institutions, universities, government agencies and corporations found that 62 percent reported intrusions.

The challenge for the students — made difficult by the lack of court-declared precedent — was to extend existing rights of citizens into cyberspace while providing effective investigative.

---

OFFICE OF PUBLIC RELATIONS
300 College Park  Dayton, Ohio 45469-1679
(937) 229-3241  (937) 229-3063 Fax
www.udayton.edu
tools and guidelines for law enforcement. The proposed code can help police, prosecutors, attorneys and judges who aren’t necessarily tech-savvy, said Brenner, an expert on criminal procedure.

The suggested code, which covers everything from definition of terms to providing for continuity of evidence and expert witnesses, is posted on the UD School of Law’s Cybercrimes Web site at http://www.cybercrimes.net/.

With a traditional search warrant — approved by a judge and specific about what evidence of crime is sought — police can enter a residence or business and physically search for that evidence. If they’re searching for stolen TVs, for example, they can’t go poking about in desk drawers or checkbook registers.

An access warrant could be the same type of tool to allow police to search computer equipment, according to the students.

"If police are searching for evidence of threats, they would need to have an access warrant that spells out their intention to do a keyword search in text files," said Brenner. "They have no reason to go into jpeg files. But if they come across a jpeg file named ‘child pornography,’ that would give them probable cause to go back to the judge and obtain a supplemental warrant to search further."

Law student Daniel Getty argued with his classmates about privilege between ISPs and their clients, and he proved his case to his colleagues. "The Internet is set up to encourage freedom of information, and nothing should inhibit that," Getty said. "The average user believes the information he or she submits to register with an ISP is confidential, e-mail communications are confidential and logs of which Web sites are visited are confidential. If clients feel the ISP isn’t keeping that information private, that would limit freedom of information on the Internet.

"One of the characteristics of privilege is a reasonable expectation of confidentiality, so I believe privilege applies to ISPs," he said. But there are exceptions. "We don’t want someone to be able to hide communications in order to commit a crime," Getty said.

Law student Jessica Rodkey worked on the section of the code that covers searches conducted without a warrant but with consent of the suspect.

"A difficult issue focused on what consent actually is and when that consent is given," she said. "For instance, is consent for search given per se by the subject when he or she consented to use a file-sharing program such as Gnutella or Napster? Our code says yes."

The students don’t expect their code to be adopted outright by law enforcement agencies across the country, but it can offer guidelines. "Ideally, our project will help to educate lawmakers and the judiciary as to the nuances and issues that this new technology encompasses," Rodkey said. "If nothing else, it will spur more dialogue in the law and technology community."

For media interviews, contact Susan Brenner at (937) 229-3794 or via e-mail at Susan.Brenner@notes.udayton.edu, Daniel Getty at (937) 435-4466 or via e-mail at gettydaf@flyernet.udayton.edu and Jessica Rodkey at (937) 296-4386 or via e-mail at jessicarodkey@hotmail.com.