DIGITALPEEPHOLES

REMOTE ACTIVATION OF WEBCAMS: TECHNOLOGY, LAW, AND POLICY

By Lori Andrews, JD, Michael Holloway, JD, and Dan Massoglia, JD

EXECUTIVE SUMMARY

The remote activation of webcams raises serious privacy concerns that existing laws do not adequately address. Webcams have transformed entertainment, medicine, home security, and many other fields. But they have also been used to spy on people in shocking ways. Currently, webcams can be remotely activated by governments, businesses, or hobbyist hackers known as "ratters," each with a distinct set of goals, but all of whom commit egregious invasions of privacy through remote activation. Hundreds of thousands of people have been the targets of surreptitious remote webcam activation, yet there has been no meaningful legislative response to the problem. Strong legal prohibitions are needed to prevent invasions of privacy by remote webcam activation.

The Constitution guarantees privacy and freedom against unreasonable searches and seizures by the government. These guarantees should preclude the government from remotely activating webcams, given that webcams are frequently located in the home, where privacy rights are at their strongest. Yet because the existing laws on government electronic surveillance allow secret proceedings and provide few opportunities for public oversight, there is no way of knowing how many times remote webcam activation has been approved by a judge, or been used without any judicial authorization. The FBI has the technological ability to activate a webcam without triggering the light meant to notify the user; yet we have no information on how many times the FBI has done so. Given the grave constitutional infirmities of remote webcam activation and the presence of less invasive alternatives, laws are needed to prevent the government from remotely activating webcams.

Businesses have engaged in shocking abuses of remote webcam activation technology. Rent-to-own stores have installed remote webcam activation capabilities on rental computers and used it to spy on their customers. Other companies sell remote access software that they activate when a computer is reported stolen, attempting to gather information on the purported thief to hand to the police. Both of these practices have led to egregious

privacy violations of innocent people. Yet because of a minimum damages requirement in the federal Computer Fraud and Abuse Act and outdated language in the Electronic Communications Privacy Act, victims of webcam spying have little recourse under federal law. Shockingly, people who have their webcams surreptitiously activated and were spied on have been held to have no recourse under the federal unauthorized access and wiretap laws.

Taking advantage of cheap and user-friendly remote access software available in the murkier corners of the internet, individual "ratters" are able to take control of victims' computers and remotely activate their webcams. Ratters, often young men, activate the webcams of their victims, often young women, and attempt to capture photos of them nude or having sex. They can then extort their victims—"slave girls," as they are often dubbed in ratter circles—for additional nude photos. They trade or even sell copies of the private images to others in their online circles. Ratters have victimized thousands of young women, including minors. While there have been successful prosecutions of prominent ratters, there is no law specifically addressing the problem of remote webcam activation.

Each of these situations demands action to prevent invasions of privacy through remote webcam activation. Given its questionable effectiveness and high level of intrusiveness, remotely activating webcams should be clearly prohibited as a law enforcement investigative technique, and the rules of criminal procedure should not be modified to encourage its uses. Private businesses should similarly be banned from employing remote webcam activation, as its supposed benefits for theft prevention and recovery do not justify the flagrant violations of privacy that inevitably occur when the technology is activated. Furthermore, federal and state law should be updated to provide a civil remedy for victims of surreptitious webcam spying. Finally, law enforcement and the judicial system should make greater efforts to prevent surreptitious webcam activation and to investigate and punish anyone who uses a webcam to violate a computer user's privacy.