Criminal Law in Cyberspace

05 January 2001
Vol. 149

Two of the most talked-about crimes of the year, the ILoveYou computer worm and the denial of service attacks on Yahoo, eBay, and E-Trade, suggest that a new form of crime is emerging: cybercrime. Thousands of these crimes occur each year, and the results are often catastrophic; in terms of economic damage, the ILoveYou worm may have been the most devastating crime in history, causing more than $11 billion in losses.

This paper asks how cybercrime is best deterred. It identifies five constraints on crime - legal sanctions, monetary perpetration cost, social norms, architecture, and physical risks - and explains how each of these constraints may be reduced by committing crime in cyberspace. The ease of cybercrime risks negative substitution effects, as offenders move away from real space and look towards the Net. Because cybercrime requires fewer resources and less investment to cause a given level of harm, the law might want to use approaches that differ somewhat from those in real space. In part, this is so because computers provide a cheaper means to perpetrate crime. Criminal law must be concerned not only with punishing crime ex post, but with creating ex ante barriers to inexpensive ways of carrying out criminal activity. For example, if computers serve as substitutes for conspirators, then law might develop doctrines that treat computers as quasi-conspirators and establish inchoate liability.

Read "Criminal Law in Cyberspace"

Contacts

Neal Katyal

Partner

> Read the full article online