LAW 7229: Legal Responses to Computer Cr

Technology has drastically changed our culture in the last twenty years. We regularly communicate on-line, transmit information about ourselves to computers at unknown locations, and keep personal data on devices in our homes an in our pockets. Large databases and worldwide connectivity afford governments new tools and methods of investigating crimes. These technologies also present ample opportunities for crime organizations to reach new victims and operate across the traditional jurisdictional boundaries of state lines and international borders. The legal landscape in this cyber world has few guideposts and presents many issues, virtually all of which are unsettled. This course will examine the rules being written so that the government can appropriately use new technology to investigate and prosecute crime. In the attempt to balance constitutional rights and effective law enforcement, is the line between government needs and privacy interests being placed appropriately? Are the criminal courts properly structured for the trial of high technology matters? The first part of the course takes up the nature of evidence gathering in the computer age. There are now vast warehouses of data, data which has been, for the most part, voluntarily supplied by the public. We will discuss the rules for accessing this information and the application of the Fourth Amendment to cyberspace, examining the statutory and case materials relating to the electronic storage of information and the various barriers raised to perceived government overreaching. The second section is an introduction to the criminal law's view of emerging technology. What are the new crimes of cyberspace and do these offenses appropriately crystallize the conscience of the community? In the couse of this discussion we will examine statutory materials and court decisions dealing with crimes such as computer hacking, spamming, stalking, pornography, gambling, economic espionage, and copyright violation. We will also take a look at the scourge of ransomware and government responses to this threat, including the impact of privacy legislation. Last we explore the particular courtroom presentation issues raised by the criminal trial of technology cases and sentencing. These issues will be examined through the lens of trade secrets and terrorism investigations and prosecutions, considering whether traditional models of discovery work in these cases, how harm is to be measured, and whether and how generational cultural perspectives should be recognized in these cases. The course also addresses the process of investigating across international borders. Exam Info: There will be an exam based on the assigned reading and in class discussion.

Credits: 2.0