Prosecution

The role of the prosecutor in the United States criminal justice system is complex. He/she has many responsibilities, the exercise of which involves him/her in several areas of criminal justice. These duties include:

1) Enforcing the law;
2) Representing the government (in criminal and civil matters);
3) Maintaining standards of conduct as a court officer;
4) Developing programs pertinent to criminal justice reform;
5) Being a spokesperson for the field of law.

"Maintaining standards of conduct as a court officer" includes the responsibility to ensure that searches for and seizure of evidence are conducted consistent with Constitutional provisions. In this respect, prosecuting cases of cybercrime is relatively new, as the form of crime itself is itself relatively new. The process of preparing a case for trial presents prosecutors with certain challenges which they have not necessarily faced before. In order to fight cybercrime, criminal evidence must be gathered from computer-based systems. This is quite different from the collection of conventional criminal evidence. The evidence consists of digital data or computer code; this evidence must be collected, stored, and presented at trial. Carrying out these procedures requires knowledge of computing technology, as well as computer forensics. Many prosecutors, particularly older prosecutors, do not have this knowledge. In Federal courts in the United States, there are attorneys who have specialized training in computer hacking and intellectual property (CHIPs). In many state and local jurisdictions, there are no prosecuting attorneys who have such expertise. An additional challenge stems from the prosecutor's having to decide if he/she has enough evidence to gain a conviction if he/she proceeds to take the case to trial. As the list of prosecutor's responsibilities above suggests, prosecutors have many and varied duties. This means they must pick and choose which cases to pursue and bring to trial.

Under these conditions, prosecutors tend to focus their time and efforts on bigger cases they know will result in successful prosecution and conviction of the suspect. Cybercrimes that have real effects on people are prioritized. These include cyber bullying, child sex crimes, single incidents that cause financial burden to a large number of people, and crimes that look to threaten the security of the country. In these cases, the evidence against the defendant is usually abundant and clearly points to his/her guilt. Faced with these facts, defendants typically enter a guilty plea to a lesser charge. Smaller crimes are not usually on the prosecutor's radar and are usually dismissed.

It should be pointed out that, even if evidence of a cybercrime is found on an individual's computer, this, in itself, is not sufficient to prove that he/she actually committed the offense. He/she can argue that 1) someone else had access to the computer and could thereby have committed the crime; or 2) the computer was part of a botnet which was used in the commission of the offense and over which he/she had no control. One defense which was used frequently in the past was the "Trojan horse" defense. The defendant would claim that his/her computer had been invaded by a Trojan horse and it was this malware that was used to commit the crime.

In order to overcome these defenses, the prosecution can point to a defendant's level of computer literacy. Someone who is knowlegeable about computer systems is likely to have a firewall and/or antivirus software installed on his/her computer and can reasonably be expected to know how to prevent Trojan horse attacks.

Another approach the prosecutor can take in a cybercrime case is to demonstrate the defendant's knowledge and intent. This is particularly relevant in child pornography cases. If a defendant's computer is found to have multiple pornographic images of children on his/her computer, records of visits to chat rooms where such pornography is exchanged, and text messages with pedophiles, this is strong evidence that the defendant intended to engage in child pornography offenses.

Some defendants have claimed a so-called "fantasy" defense. This occurs when a defendant accused of attempting a crime (enticing minors into sexual activity, for example) claims that he/she never intended to complete the crime. Instead, they claim they were engaged in a fantasy and, in the case of luring a minor, believed they were dealing with an adult.

In general, the most effective way to respond to various cybercrime defenses is to conduct a careful and thorough forensic examination of a defendant's computer. This will reveal the contents of the defendant's machine, with special attention paid to any malware on the device, how it works, and any other "suspicious" data or files on the device. [Of course, such a search should be conducted with a proper search warrant (4th Amendment) and, if any of the data are encrypted, in accordance with the 5th Amendment.]

In those cases which go to trial, jurors are developing better understanding of computing technology and how it works. This fact in itself is not necessarily for the benefit of the prosecution or defense. In some cases, jurors have acquitted defendants , while in others, they have convicted defendants.

In some jurisdictions, there is an additional consideration by prosecutors which effects their selection of cases to try. Where the prosecutor is an elected official, he/she may be concerned about re-election. In other areas, the prosecutor may have aspirations to seek a higher office- perhaps mayor, governor, or Federal Representative or Senator. In either case, he/she may choose high profile murder or sexual assault cases to take to trial because they receive attention in the media. Many cybercrimes can seem esoteric and difficult to understand; these offenses are likely to be dismissed by prosecutors who have their eyes on elective office.