

PROSECUTING INTERNET CYBERFRAUD IN THE FUTURE

Article

By

**Michael Donovan, Chief
Bureau of Investigation
San Bernardino County District Attorney's Office**

Command College Class XXXI

Sacramento, California

November 2001

IDENTIFYING THE ISSUE

The Internet was developed in the 1960's by a United States governmental agency known as the Advanced Research Projects Agency (ARPA) as a method for universities to communicate with governmental entities regarding weapons research.¹ A key component of the communications network was its redundancy, based on the premise that the communications system could survive in case of nuclear war. The network was able to search communication cables and computers for an expedient method that would guarantee successful communication. If the most direct pathway was too congested or had ceased to exist, such as having the lines cut during a wartime event, the network would simply reroute the communication effort through a different set of cables that would ensure the data reached its destination.²

The introduction of the Internet for business and personal use saw an explosion of cyber crimes taking place via the Internet. Bulletin boards gave way to web sites and e-mail. By the mid-1990's personal computers were in one out of four homes in the United States. Cyber criminals upgraded their abilities and began terrorizing websites by changing their content or by redirecting the inquiries sent to their web site to a false site established by the hacker. From here, it was a small step to gain access to stolen data and perpetrate vast financial crimes. The theft of information from corporate computers became widespread.

Federal agencies, state agencies and larger local agencies began steps to train law enforcement officials in how to investigate criminal activity involving the Internet, and how to determine the identities of the perpetrators of the cyber crimes. Criminal statutes were written to address utilizing computers to commit criminal acts, and to seize the

equipment utilized by the cyber criminals to commit their activities. More and more officers attended courses on computer crime and their understanding of conducting the investigations grew.

As officials began to understand how cyber criminals behaved, and how they committed their crimes, gathering evidence to prove the crimes while identifying the criminals became more difficult. Freedom of speech advocates created a website that specialized in providing anonymity to those who desired it. With no requirement that a person using an e-mail account pay a fee or actually disclose his or her true identity, ferreting out cyber criminals became more difficult. Additionally, law enforcement officials began to ask who pays for the cost of the investigations and the equipment necessary to conduct the investigations.

While law enforcement officials were busy investigating child-focused criminal activity, another area of cyber crime was virtually exploding: cyberfraud. In cyberfraud cases, large dollar losses are investigated because of the impact such thefts have on our society. In this paper, the focus is not the large case, but rather the economics, logistics and legislation of conducting interstate cyberfraud prosecutions.

The result of this inability to successfully combat interstate cyberfraud at the local level has been to grant cyber criminals the ability to commit cyber fraud with virtual impunity provided the crimes are committed across state lines. There are no laws that exist which allow local or state officials in one state to prosecute a criminal in another state for the commission of crimes that generated in a different state. For example, if a cyber criminal in Maine sells a Rolex watch over an Internet auction site to a buyer in California, no state criminal statutes have been broken. If once the buyer has paid for the

watch, and the watch that arrives from Maine in California is determined to be a fake Rolex, then a criminal act has occurred.

The issue at hand is that interstate cyberfraud is largely ignored now, except in large federal investigations. This allows common thieves to operate in a high tech environment with virtual impunity. There is no denying that computers are a part of everyday life, and that in the future, more computers will be put into use. With the growing popularity of the Internet, and the increasing speed at which technology performs, more and more criminals will be taking to the Internet to conduct their transactions. As evidence of this, all one has to do is look at the rate at which public telephones are disappearing, and the number of adults and children who now have a cellular telephone pressed to their ear. Technology is being embraced at an ever-increasing pace. By developing a plan to address interstate cyberfraud, our citizens can be better protected while ensuring criminals will have to answer for their misdeeds.

NOMINAL GROUP TECHNIQUE

In order to develop a model strategic plan and identify and measure possible trends and events, the Nominal Group Technique (NGT) was utilized. This technique is used to assist in the creation and management of a desirable future with respect to particular issues. The panel consisted of an Assistant District Attorney, a Deputy Chief of Police, a Supervising District Attorney Investigator, an FBI Agent, and a computer technology supervisor.

This panel discussed the issue of cyber fraud and developed events and trends which were used to create a probable future scenario depicting how interstate cyberfraud would be prosecuted in 2006. The information developed by the panel

demonstrated that several trends and potential events called for action by way of legislation that will enable the introduction of technology into courtroom environments and will facilitate the investigation of and prosecution of interstate cyberfraud.

EXISTING CALIFORNIA LAW

There are very limited times wherein closed circuit television may be utilized to obtain the testimony of a witness in a California criminal matter. According to California law, certain children who are victims of sexual assault may testify via closed circuit television.³ It is a logical inference to extrapolate the use of closed circuit television into the use of a high definition video conferencing system. Therefore, there is some lawfulness of using live video testimony in California, and the ability to modify this statute or expand the usefulness of this technology by new legislation exists. Such an expansion could provide for the use of this technology in other matters where witnesses resided in states outside of California.

TRANSITION MANAGEMENT

In order to develop a Transition Management Plan, certain stakeholders must provide active support to ensure success. These stakeholders were identified as: Elected Federal Officials, Elected State Officials, Elected City and County Officials, Federal Bureau of Investigation, Citizens of the United States, Professional Associations, Peace Officers, Criminal Defense Attorneys, County, State and Federal Prosecutors and State and Federal Judges.

A detailed Transition Management Plan cannot be finalized without buy-in from the aforementioned stakeholders, and effective mitigation of snaildarters. In order to ensure the successful development of such a plan, the requisites of the Transition Management Plan must include the following elements: Develop an oversight committee, identify the

present state of the issue, identify the future state of the issue, determine what changes need to be accomplished, facilitate an environment in which stakeholders are prepared to accept change and develop a communication plan.

BUDGETARY IMPLICATIONS

To equip every county in the country with a cyber courtroom that is high definition video conferencing capable will cost billions of dollars. To purchase equipment, train and fund the salaries and overhead of a squad of cyber cops for every county in the nation will cost more billions than equipping the cyber courtrooms. Make no mistake, the ability to develop the infrastructure and purchase the equipment to investigate and prosecute interstate cyberfraud hangs on the oversight committee's ability to develop a stable funding mechanism. This funding must be from broad based sources, and must have minimal impact on governmental and consumer budgets. Industry will be unwilling to pay additional taxes, and consumers will be very wary of advancing funds to the government for a service many believe should be provided without additional charge as a safety benefit to the public.

Developing a successful legislative package will be relatively simple in contrast to the designing of a comprehensive funding mechanism for interstate cyberfraud prosecution. Raiding existing special interest funds will be unsuccessful, and therefore, new sources of funding must be developed. Perhaps the easiest and least painful mechanism to employ is a national user tax for Internet service. Appropriate lobbying efforts, advertising and public relations will necessarily be the cornerstone of developing a sustainable revenue stream to fund these efforts. Much consideration must be given to developing a funding package, and operatives at the highest level will need to be involved in this process.

RECOMMENDATIONS

To adequately address interstate cyberfraud, a multi-pronged approach must be adopted. Fastidious attention to both the big picture and the details must occur in order to interweave a viable product that will be consumed without remorse. This approach should include:

- Adapting the Interstate Witness Compact to allow for out of state witnesses to testify via high definition video conferencing systems from court facilities that are in close proximity to their home or office. This will make the cost of prosecuting interstate cyberfraud much more reasonable and will pave the way to use similar testimony in other arenas after the system has proven its value.
- Establishing a system of cross-designation for law enforcement authorities assigned to investigate interstate cyberfraud. This will allow for officials to have the legal authority to investigate and enforce cyber crimes that cross state lines. Such cross-designation will require new laws at the state and federal level.
- Training law enforcement officials and establishing true multi-jurisdictional task forces to address the increasing threat of interstate cyberfraud. Local, state and federal law enforcement officers, as well as computer professionals will populate these task forces. Technicians who have a firm grasp on present and future technology will also be utilized.

CONCLUSION

Although cyberfraud activities are relatively new, any analysis that is done by a layman will quickly identify that cyberfraud is really nothing more than a high tech con game. Criminals have come of age and learned to use technology to separate generally innocent victims from their legitimate earnings. Face-to-face meetings are no longer

required in order to engender trust between a con man and his target. Close proximity is also no longer a variable in this criminal equation.

Law enforcement agencies must act quickly before the game is over and the interstate cyberfraud swindles so pervasive that the proverbial barn door is incapable of being closed. Technology has erased geopolitical boundaries, however our laws have failed to keep pace. Only fast acting leadership will be able to close the gap created and exploited by cyber criminals.

Law enforcement does not traditionally hire computer experts, nor does the average peace officer or detective consider fraud a meat and potatoes type of criminal activity. Law enforcement is also traditionally unwilling to share information or glory (successes) with other local, state or federal agencies. In the world of cyberfraud, beliefs, hiring practices and closed-mindedness collide with disastrous consequences. In order to successfully combat and prosecute cyberfraud, law enforcement officials must pull together, put their differences aside, and commit to working together as a team dedicated toward successfully implementing a cohesive, inclusive plan that effectively targets cyber criminals. Such synergy is imperative to success.⁴

Though not a panacea, development of the ability to prosecute interstate cyberfraud will lead to the next logical step of prosecuting international cyberfraud. Law enforcement has the ability to address interstate cyberfraud now. The technology and training is available, and long-term funding can be secured. If law enforcement fails to act, to become captains of its own cyber destiny, then law enforcement will no doubt one day become slaves to cyber terrorism by virtue of its own inaction. Law enforcement can be proactive, or reactive. Law enforcement leaders can wait for someone else to take up the charge, or they can set about to change the world. These plans must be acted upon so

that law enforcement officials can shape providence, rather than have a probable dismal destiny thrust down their throats.

Left to our own devices and absent willing leadership, interstate cyberfraud prosecution capabilities for local and state agencies will remain a dream. A team approach to tackling the issue of interstate cyberfraud prosecution is required, and representatives from local, state and national law enforcement agencies are mandatory committee members for any oversight team responsible for development and implementation of this plan. Individual state or local agencies lack the capacity to ramrod an operation of such scope. The implications of developing the ability to prosecute interstate cyberfraud is such a potential logistical nightmare, that only a very large organization with access to incredible resources and manpower pools has the opportunity to successfully develop and implement the plan presented here.

One organization meets the size and interest requirements necessary to undertake such a mammoth operation. The International Association of Chief's of Police (IACP) represents thousands of police administrators in every region of the country, as well as in virtually every nation in the world. IACP is a logical organization to look to for the leadership necessary to establish a credible voice at all levels. IACP is an entity with substantial credentials as well as international membership. IACP can ensure that such an undertaking to develop the real ability to prosecute interstate cyberfraud at local, state and eventually international levels is given the credibility it requires in order to succeed. Accordingly, IACP should lead the charge to develop, implement and maintain the ability of state and local law enforcement entities to prosecute interstate cyberfraud.

¹ Encarta Encyclopedia on-line [<http://encarta.msn.com>], accessed June 12, 2001.

² Ibid.

³ California Penal Code § 1347.

⁴ Covey, Stephen R. *Principle-Centered Leadership*, Simon & Schuster, 1991, p. 46.

Bibliography

- California Penal Code, 2001 version. New York, NY. Lexis Publishing.
- Covey, Stephen R. 1991. Principle-Centered Leadership. New York, NY. Simon & Schuster, Inc.
- Frank, Mari and Givens, Beth. 1999. Privacy Privacy!. Office Depot Publishing.
- Hackleman, James B. Personal interview. San Bernardino, California. May 9, 2001.
- Hyman, Cletus. Personal interview. San Bernardino, California. April 13, 2001.
- Morgester, Robert. Personal interview. Sacramento, California. April 12, 1999.
- Morgester, Robert. Personal interview. Sacramento, California. March 16, 2001.
- Osborne, David and Gaebler, Ted. 1993. Reinventing Government. New York, New York. Plume Publishing.
- Phillips, Donald T. 1997. The Founding Fathers on Leadership. New York, NY. Time Warner, Inc.
- Rosenblatt, Kenneth S. 1991. High Technology Crime. San Jose, California. KSK Publications.
- Stout, Dennis L. Personal interview. San Bernardino, California. April 11, 2001.