Emerging technology

Technology

Introduction Since computers have become such a big part of our lives It Is no surprise that even criminals now know how to hack into large computer networks. Obtaining electronic evidence may be one of the most difficult types of evidence to recover. Another issue is authenticating this evidence; however with the help of legal standards this evidence Is admissible In court today. Even though computers are the most dominant form of technology that is used in a variety of situations, there are set backs to everything and computers are no exceptions as this paper will explain (Forensic

Science, n. D.). The Advantages of Computers and the Use of Computer Technology in Investigations In order to paint an accurate picture of the advantages of computers and technology relating to investigation we must start as close to the beginning as possible. This would be when President Johnson in his State of the union Address to Congress in 1968. This is where the President made the announcement " to bring the most advanced technology to the war on crime In every city and country In America" (Northrop, 1993).

It was less than ten months when the congress along with he President, put into law the Omnibus Crime Control and Safe Streets Act of 1968. This law created the Law Enforcement Assistance Association (LEA), to handle and deliver on the promise of the President of technological assistance. During the next ten years the LEA contributed meanly $50 million to state and local government criminal Justice and law enforcement agencies for crime fighting. Other federal agencies like the FBI matched the funding as well as local and state governments themselves (Northrop, 1993).

To demonstrate the usefulness of computers by police In the fight against crime, this pare to the paper will refer to results from a comprehensive repeated-measures field study that looked specifically at how useful computers are to police in the fight against crime. The study focused on a particular class of computer use, which was the searches for vital information because this is the bulk of computer activity for officers and are valued by the police In their fight against crime. Between 1 976 and 1988 the data did " show a clear Improvement In both the use of and benefits from such systems" (Northrop, 1993).

The only drawback 1 OFF Alice effectiveness is badly constrained by inadequate training of patrol officers and detectives" (Northrop, 1993). However, there is a very simple solution to this small glitch and that is to create an adequate training system and put all officers through that training program (Northrop, 1993). The most notable problem facing officers was the chronic lack of information. This spans the range from the police chiefs shortage of information on how to use the departments limited resources to the patrol officers uncertainty over whom to stop and question regarding suspicious behavior.

In the ass's and early ass's, this problem was addressed using a multi-facade management approach and there were big payoffs. The problem of improving how information was provided to police officers in the street or to the detective working a case was harder to fix. They soon realized the only way to specific individuals or cases was the existing records. However, the only means of utilizing those records was to look them up (Northrop, 1993).

From utilizing computers in cars so officers could run a license plate and social security number to see if there are any warrants out for the errors they stopped, to more advances such as carrying cell phones, GAPS tracking systems in cars, crime mapping tools, information sharing between state and local law enforcement, to even sharing information across countries. Technology has come a long way in helping officers and other agents within the criminal Justice system do their Job. Just a bit more about the advantages of the things mentioned above and time to move on.

The most interesting thing is Geographic Information Systems (GIS), which has become a most important tool for law enforcement agencies. GIS, other mapping software and desktop computers now are capable of mapping and data analysis that is way above and beyond what used to be possible with backroom mainframe computers (Rubble, 2011). Another great advancement is the widespread use of everyone using mobile devices. Many officers now use two to three cell phones. The invention of APS has made it easy for everyone to tap a button and instantly retrieve valuable information.

Information that used to take several steps to obtain using a browser is now at the officer's fingertips. Mobile technology is evolving al the time and it is evolving fast, even in the past few years the government has been able to identify a suspect through a facial recognition app on the phone, look up a potential Jurors social media profile during over dire, and now they even have real time data streaming to mobile devices which can provide information on a fugitive or get instant news feeds. There is no doubt that computers and technology have taken law enforcement to a whole new level (Rubble, 2011).

What Disadvantages Face Law Enforcement with Respect to the Advancements of Computers? One big equidistant is that there is such a high volume of information being exchanged daily on the internet and while this is a convenient thing for most of us, there are also criminals taking advantage of the opportunity. There is corporate fraud, theft, intellectual property disputes, and even breach of contract and asset recovery issues. These are some of the situations that use computers to commit the crime and use computer forensics to solve the crime (n. A. , 2009).

An additional disadvantage is making sure that the digital evidence is going to be admissible in court. Since data an be modified very easy, the analyst must be able to comply with the standards of evidence required by law. The analyst must make sure their investigation is fully the data. Computer forensic experts are hired by the hour and the process of analyzing and reporting the data can take up to 15 hours depending on the nature of the case (n. A. , 2009). Other disadvantages are really the same ones facing all users of technology. If the system is down there is no information that can be retrieved.

If the user is not trained in using the technological equipment at his/her disposal then this will be a waste of time. If the input of information is incorrect which sometimes occurs because of human error, then that will cause a problem for officers in the long run. The Case Chosen to be researched where the Computer was used to Aid in the Commission off Crime. 3 NJ Students Charged in School Computer Hacking On April 14, 2010, in Hatfield N. J. Three students hacked into one of the top performing High

Schools. They are now facing charges for attempting to change their grades once they were into the system.

The three students are boys, ages 14, 15, and 16 but because they are minors their names have not been released. The Boys were found out when a staff member found one of the boys using keystroke capture software on one of the computers at the school in an attempt to steal a teacher's password. That student then implicated the others in this crime. The boys were charged with illegally obtaining information and were released to their parents (Associated Press, 2010). This is a wonderful example of how people, who might never have committed a crime in their lives, get ideas about computers as if this is not a crime.

They get on the internet, explore places and things that are illegal and never hind twice about it because they are either in their own home and feel protected, or they feel that it is easier to get away with computer related crimes and take their chances. There is too much technology and it is dangerous in the wrong hands. People need to realize that especially crime on the internet will always be solved sooner or later because what you do on a computer leaves a print forever that can never be erased.

Research Case Where a Computer was Beneficial to the Prosecution in a Criminal Case In this case a woman age 45, named Sonic Martin, from Nigeria ND Chicago, Illinois was " manager of a Chicago cell in one of the most sophisticated and organized computer hacking and ATM cash out schemes ever perpetrated" (U. S. Attorneys Office, 2012). On August 12, 2012 she was sentenced to serve two years and six months in a federal

prison on charges of conspiracy to commit wore fraud. She will also serve five years of supervised release and $89, 120. 5 in restitution fees (U. S. Attorneys Office, 2012). According the United States attorney Yates, in November of 2008 a group of hackers obtained unauthorized access into the computer system f a company called Wordplay US, Inc. , then known as ORBS Wordplay, which is a payment processor in Atlanta. The hackers were very sophisticated and used some daring techniques to compromise the data encryption that Wordplay used to protect the customers data on payroll debit cards. These are used by more and more companies to pay their employees.

This is convenient for employees as they can use the debit card right away or use it to withdraw their salaries right from an ATM (U. S. Attorneys Office, 2012). Once they were in, hackers raised the balances and ATM withdraw limits on the compromised accounts. They then provided a network of lead " cashers" with 44 debit card account numbers and their PIN numbers, which they used to withdraw more than $9 million from over 2, 100 ATM; s in at least 280 cities Kong, Japan, and Canada" (U. S. Attorneys Office, 2012).

The whole thing, $9 million dollars, took less than 12 hours to pull off on November 8, 2008 (U. S. Attorneys Office, 2012). Throughout the cash out the hackers monitored these fraudulent ATM withdraws in real-time from inside the computer systems of Wordplay. Once the transactions were complete the hackers sought to destroy data stored on the card recessing network so they could cover up this illegal activity. Wordplay discovered the unauthorized activity and reported the breach (U. S. Attorneys Office, 2012).

Sonic Martin was working with one of the lead cashers and supervised a cashing crew in Chicago. Martin was given PIN codes, and payroll cards, and then manufactured counterfeit debit cards based on that information. So she handed out cards to her underlings that she recruited and supervised. Together they all withdrew approximately $80, 000 from various Tam's around Chicago, during the early morning hours of November 8, 2008. Martin's primary address is Nigeria (U. S. Attorneys Office, 2012). This case was investigated by special agents of the federal bureau of investigations.

Other who helped provide assistance included; numerous domestic and international law enforcement partners and Wordplay immediately reported the crime and substantially assisted in the investigation (U. S. Attorneys Office, 2012). Conclusion My belief is that the new technology and computers have really given law enforcement some spectacular tools to do their Job. I feel that technology has aided in the increase of incarcerations. Anytime criminals can be taken off the streets or even out of the darkness of their homes where they are committing crimes, this is a good thing.

Yes there are some disadvantages that can also be dealt with. The problems of officers being unaware of how to use some of this modern technology can be cured by sending them to some training programs. All officers need to be aware of what evidence to collect when it is possibly on a computer and the chain of custody that this type of technology requires. As technology advances, unfortunately so will the crime that is being committed with that technology. Officers everywhere just be able to respond to these crimes effectively.