Joshua Garris

April 19, 2010

The Evolving World of Computer Security and Laws

Computers are being used in everyday life more and more. The problem with the increasing use of computers in everyday life makes it harder for security to catch up. Information security is a major issue all around the world because of the risk of valuable information getting stolen and misused. It's such a major issue that countries and business spend billions of dollars to make their networks secure, but all IT professionals know that security is only affective when they see an attack happen and then learn ways to prevent it. Just like the United States view on computers with their "we'll see it as it comes" strategy on computer security and laws. As the crimes are committed then the court cases are used to define the laws that we have now by their rulings.

To help protect its on citizen's from unlawful searches and seizures in the United States is the fourth Amendment rights. The case ***WARSHAK vs. United States*** asked this question if e-mails required a warrant, to seize all of a person's data from a third party. Warshak was under investigation from the federal government for mail and wire fraud, money laundering, and related federal offenses. The courts obtained an order to the internet service provider (ISP), NuVox Communications to turn over all information pertaining to Warshak's e-mails accounts with NuVox. Included with this information was Warshak's customer account information, billing information to include banking accounts. This was all done with a court order, using the Stored Communications Act. Warshak sued under the justification that his fourth amendment rights were violated. As the cases preceded the government tried to say that e-mail or any data held by a third party like an ISP, the defendant wavered all his rights to privacy. The judge threw this reasoning out because he used the telephone companies as an example. Just because two people talk on the phone, there is a sense of privacy in the conversation even though it goes through a third party which is the telephone companies. Then the federal government made the argument that since business were creating programs to search e-mails for child pornography that Warshak's privacy with the ISP was invalid. The judge ruled against this because the search was done by a program and not by a human being. Since it was not done by a human then there is a sense of privacy. Since the federal government could not come up with a good argument why Warshak's right to privacy was invalid, Warshak won the case. This case was very important because it established a business and a customer's right to privacy and that a business doing a scan on their system for any reason could not compromise their customer's privacies. What this does for the customer is their right to be protected from their information, such as e-mail and data, contained by a third party to be protected.

There is a limit to this case though with the use of programs. China has an elaborate filtering system in their counties which is nicknames "The Great Firewall" (Byron, 2010). They use thousand of programs to hack into and probe computers for information in their countries and this has cause huge problems with Google. Matters gotten even worst when business and countries started to get hacking attempts all originating from China (Moyer, 2010). The hacking and filter got so bad that Google made the decision to pull out of China.

There are also attacks from within the United States that have been used to prove the consequences of hacking. In the case of ***U.S. vs. Arabo***, a business man by the name of Jason Salah Arabo, attempted to hack thousands of computers using a bot program in order to crash his competitor's websites. This showed how computers are being abused by competing business to attack one another. Arabo lost his case and was fined for $504,495 dollars. In the case of ***U.S. vs. Kwak***, Ancheta hacked thousand of computers which then turned them into zombies. These zombies then turned around and hacked other computers. Ancheta took this massive army and sold the control over them for about $3,000. Ancheta then took this massive army and used it to launch denial of service attacks on servers and to send spam. It got so bad that the program Ancheta wrote affected defense networks of the United States. Ancheta was sentenced to 57 mounths in federal prison and fined for $15,000 for the damaged systems of the government computers. These two cases show you the cost of hackers take and the outcome of their events which are normally not good. The Law that was able to punish these hackers was the Computer Fraud Abuse Act, which helps protect citizens from hackers. Also it protects people computer from harm of a hacker and the information on it. There was once hacker that created a lot of harm to a hospital. ***U.S. vs. Maxwell***, caused harm to the computers to a hospital which in turn risk the medical health to the patients. The botnet affected the hospital computer system so much that door would not open and computer systems in the intensive care units were shutting down. Maxwell is facing fines up to 10 year and fines up to $250,000 (U.S. vs. Maxwell, 2006). These cases show you the need for information security but also the difficulty in preventing them. Since new ways of hacking are being invented and Security administrators are playing catch up. Even the federal government is immune to hackers.

U.S. vs. McCarty is an example of an employee who is using his power over a system to abuse the system. McCarty was a network administrator for the University of Southern California. While he was working on the USC's on-line applicant website, when he notice there was flaw in the system. The flaw allowed him to change any applicant's data such as social security numbers and birth dates. McCarty created a program to hack into the system and take several students applications. After McCarty did this he created an email to ihackedusc@gmail.com and bragged to securityfocus.com (U.S. vs. McCarty, 2006). Security focus told the school about the vulnerability. McCarty only got caught because the Federal Bureau of Investigation traced the internet protocol number on his home computer. He is faced up to 10 years in federal prison. This shows that when taking security into account even the people in charge are at risk of abusing the system. The only way for a business or a university to protect themselves would to get trusted people to protect their system and to check up on the people to make sure they are doing their job.

There is one flaw that is a constant threat to business, is keyloggers. In ***<u>U.S. vs. Jiang</u>***, Jiang admitted that he installed several keylogging software on computer terminals located at kinko's stores. What the keylogger did was record the keystrokes of users, to steal their passwords and user names. This happened for several months, which then Jiang used this data to try and hack into the user's bank accounts. The courts gave him 27 months of imprisonment and $201.620 in fines (U.S. vs. Jiang, 2005). That was not all that Jiang did, he also sold online 2,000 copies of Microsoft Office 2000 Professional Edition (U.S. vs. Jiang, 2005). In one famous case is with ***<u>U.S. vs. Levine</u>***, Where Scott Levine, used his company Snipermail, to steal thousands of customers records. He used their e-mail and bank accounts and sold them off to a broker. To obtain this information Levine used software that looked up user names and passwords to later sell. During the court case Brian Marr, a U.S. Secret Service agent said

> "Neither the Internet nor cyberspace will ever be a safe haven for individuals who attempt this type of cyber crime. The Secret Service, along with our law enforcement partners, will hunt you down, keystroke by keystroke, until you face a jury of your peers. The Secret Service's investigation regarding this type of crime has been and will always be a top priority(U.S. vs. Levine, 2006)."

So for a Business to protect itself to the fullest will have to use top security, and help keep its personal in check while they wait for government laws to catch up to the times. These future laws will help protect them and their customer from a wide range of crime and theft that has gone high tech. As all administrators know that, they have to constantly look at new ways to hack systems to stop them in the future while keeping their systems safe.

Joshua Garris

April 19, 2010

Bibliography

Byron, Acohido. "Google cracks door to secrets." *USA Today* n.d.: *Academic Search Premier*. EBSCO. Web. 19 Apr. 2010.

Moyer, Michael. "Internet Ideology War." *Scientific American* 302.4 (2010): 14-16. *Academic Search Premier*. EBSCO. Web. 19 Apr. 2010.

U.S. vs. Ancheta, 06-051 (C.D. Cal.)

U.S. vs. Arabo, (D. N.J.) August 25, 2006

U.S. vs. Jiang, 05-39 (S.D. N.Y.)

U.S. vs. Kwak, 06-285 (D. D.C.)

U.S. vs Levine, 06-008 (E.D. Ark)

U.S. vs. Maxwell, (W.D. Wash)

U.S. vs. McCarty, 06-045 (C.D. Cal.)

Warshak vs. United States, 490 F.3d 455 (S.D. OH)