Global Information Assurance Certification Paper

Security and Privacy Rights

Matthew Wagner

October 07, 2002

Abstract

Security and privacy share the same common goal of freedom. Privacy has its roots in the protection of unsanctioned intrusion, while security is the tool that protects us from harm. Technology has changed the way we work, communicate, and the quality of life we lead, but does it also has the ability to infringe upon our belief of what material is private. The affinity we have towards automation and innovation may have grave consequences. Individual rights have been the challenged more in the age of technology than ever before because of the wealth of information captured and stored. I will discuss recent laws passed to protect the rights of individuals as well as to protect the safety of a nation. I will discuss tools used to ensure information is kept private and how those tools can have grave consequences.

Introduction

Does the information you send over the phone or data lines belong to you once it has left your house, or is it property of the government? The National Security Agency currently has the ability to browse and intercept any information they believe it is a threat to national security even if you encrypt the information. If a citizen of the United States decides to write a program that encrypts their data, they cannot transfer that encryption over the United States borders without the consent of the National Security Agency. If they transfer encrypted data without consent they can be arrested and punished as a terrorist. The American Civil Liberties Union advocates that the information sent over phone and data lines are protected by the Bill of Rights and to allow government to eavesdrop would violate our 1st Amendment right of freedom of speech. The ACLU states that by allowing government to readily decrypt information the individual looses their guarantee against unreasonable searches and seizures that is protected by the 4th Amendment in the Bill of Rights. The National Security Agency along with other various Intelligence agencies are charged with protecting National interests that include the monitoring of phone and data lines. Scott Charney of the Department of Justice's Computer Crime Division is already on record as to his conviction that cryptography is a top-priority problem for law enforcement. He has called the spread of unbreakable encryption a serious threat to "law enforcement's ability to do its job." (Godwin). Immediately following the September 11 attacks Attorney General John Ashcroft presented several new pieces of legislation intended to aid the FBI, NSA and DOJ in the combat against terrorism (Sondreal). Has the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" or the USA PATRIOT Act created a slippery slope by allowing government agencies like the Department of Justice greater latitude in the collection of intelligence, or should government play a larger role in the

monitoring of all domestic communication? What options do we have to ensure the electronic data we send is kept private?

What guarantees our Privacy?

What makes an American free? When asked to describe what guarantees ones freedom, The United States Constitution and the Bill of Rights are quickly offered as the binding document between citizen and the United States government. Do these documents ensure privacy on the phone or using the Internet? Since the acts of terror on the World Trade Center and the Pentagon on September 11, 2001, President George Bush Jr. has requested for more intrusive eavesdropping techniques like roaming wiretaps and sharing data collected by separate government agencies to prevent acts of terror. Intelligence agencies were accused of not ensuring national security shortly after the attacks. The Department of Justice was quick to point out that while collectively the agencies had information on the terrorist, by law the agencies are not allowed to access other agencies files. This means that the Federal Bureau of Investigation does not have the ability to read information collected by the Central Intelligence Agency and visa versa. These agencies also noted that obtaining the necessary paperwork to initiate surveillance is cumbersome and this often allows criminals the upper hand in evading law enforcement. What lengths should government pursued to ensure the American way is protected? The crux of the matter lies within defining what rights are protected by the Constitution and the Bill of Rights. The question we are faced with is should civil liberties be placed before national security.

What do the 1st and 4th Amendments state about privacy?

The 1st Amendment states "Congress shall make no law respecting an establishment of religion, or prohibiting the fee exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances" (Holmes). Does a citizen run the risk of being labeled a traitor, or do they hold dangerous material by merely possessing a dissenting view of the government? Referring to our founding fathers "They believed these rights could not be taken away, even by government" (Holmes). Since our founding fathers wrote our Constitution and Bill of Rights from a philosophical perspective we must infer much of present day issues from the underlined meaning of the original text. The framers of the Constitution were acutely conscious of the risk associated with majoritarianism and therefore created the Constitution with many "checks and balances" (Godwin). This is to ensure that government does not tread on the rights of the people it represents and become a dictatorship. The topic of privacy over the Internet is the challenging the fundamentals set forth by the Bill of Rights, but the fundamentals behind ensuring privacy aren't new. Does a citizen run the risk of being labeled a traitor, or do they hold dangerous material by merely possessing a dissenting view of the government?

The Amendments were mindfully constructed to protect the privacy of the citizen from their government. The 4th Amendment ensures that citizens are protected against unreasonable searches and that no seizure may be permitted without probable cause. National security wiretap requests go to a secret court that meets in camera and never issues opinions (Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1802(a) (1988)). Title 18 of the U.S. Code also permits warrant less surveillance in emergency situations involving immediate danger, death, or serious physical injury to any persons; conspiratorial activities threatening the national interest; or conspiratorial activities characteristic of organized crime. U.S.C. § 2518(7) (1988). This allows government to ultimately decide for the individuals what is best rather than the democratic method prescribed by the Constitution and the Bill of Rights. President George W. Bush has recently asked Congress to allow for roving wiretaps on the persons living within the borders of the United States via the USAPA. A taboo topic before the September 11, 2001 acts of terrorism. What the President is asking for is that all restrictions on the issuance of warrants for wiretaps be lifted so that the policing official are not restricted to placing a wiretap on one phone, or for a set period of time. Rather, the individual would be under surveillance no matter what device they use or where they travel. This would mean that if information is unintentionally collected on other individuals during the tap, then that information becomes admissible in court. This is a direct violation of the 5th Amendment that states that no person may witness against himself. Password, key codes, pin numbers are all common terms that foster a sense of safety amongst society. They ensure us that our sensitive information can only be read by us. I can mail a letter to my father with less threat of a secondary party reading the contents than I can by send him an email. The future holds the ability to pinpoint the vary time and location of an individual based upon their secure communications. This is done every time we make a call on a cell phone, use our credit card, or send an email. The true threat to national security is giving government the ability to place its citizens under surveillance.

Encryption Standard

Encryption is a method that translates readable information into a form that is not with decryption acting as the translator of the encrypted data (Peha). The fundamentals behind encryption can be dated back as early as the 18th century, so why didn't the Constitution include cryptography? The answer might be that most of the official documents that an individual possessed were kept within the boundaries of their homes. The 4th Amendment guarantees that government could not search the premises without a search warrant and probable cause; the rights of the citizen were upheld. Does government then have the right to search document that are transferred over voice and data lines? If I send a secure online transaction between an online store and my bank the government reserves the right to read and store the data that I have transmitted if they believe I am involved in any criminal activity. Prior to the USA PATRIOT Act of 2001, the Department of Justice was under guidelines similar to that of the wiretap policy when decoding encrypted messages outlined in by the "Wiretap Statute" (Title III 18 USC 2510-22). They must first

obtain a warrant to gather information on your transactions and the tap may only last for a finite period of time. This policy dictates what steps must be performed to obtain a warrant. The USA PATRIOT Act under Section 209 affords government the right to gather information without a warrant if they feel that National Security is at risk, or that information might be compromised. This allows the government the liberty to monitor any individual that they choose based upon the criteria of "reasonable" searches. The term “reasonable” is ultimately determined by the law enforcement agent and not a court, or judge. The USAPA is designed “To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigative tools, and for other purposes.” (Sondreal). Prior to the USAPA, an Internet Service Provider (ISP) could not release information regarding a customers’ personal information, including IP address and financial information, without a court order. Under this act the information can now be released from the ISP voluntarily (Sondreal). The Omnibus Crime Control and Safe Streets Act of 1968, allow for “emergency” wiretapping, however, a request for a court order must be made within 48 hours of said wiretapping. The USAPA extends, to 90 days, the time requirement for requesting the court order and judges are no longer permitted to deny the requests (Sondreal).

In the early 1970’s, the National Bureau of Standards decided to define a national standard cryptographic algorithm (History Channel). Prior to that standard, corporations were using various types of encryption, but were experiencing compatibility issues while sharing data. Corporations looked to the government, who regulates the telecommunication standards, to determined one cryptographic product. That cryptographic algorithm was developed by IBM and was originally a 128-bit encryption package. The National Security Agency after reviewing the algorithm decided to support the smaller 56-bit algorithm. The critics of the smaller algorithm believed that it was adopted as the standard because the NSA could easily decode the messages. It was also rumored that the NSA requested that a “back door” be implanted in the algorithm to allow the NSA the ability to quickly and easily decode the encrypted data (Froomkin). This allowed the NSA the ability to read virtually all information that was under the guise being a secure transmission. The NSA not only dictated what the standard would be, it also control who is able to send secure transmission from the United States to other countries. The NSA is the governing body that either grants or denies corporations the ability to transmit encrypted messages, and to do so without permission can be tried as a Federal offense.

Encryption for the people

Encryption can protect personal privacy rights when it is applied to medical records, spending histories, and credit ratings. Government agencies can protect sensitive and information from foreign governments. Encryption can protect critical civilian infrastructure, such as banking systems, telephone network, electrical power grid, and air traffic control systems from vandals and terrorists. Encryption can even address fraud, tax evasion, identity theft, and other information-based crimes of the

rising electronic marketplace (Peha). Why might this be dangerous? Without data encryption the information about ones spending history at your local grocery stores can easily be sold to insurance agencies or marketing companies to create a profile. Companies like Metromail who is owned by Experian used prisoners to enter personal information from surveys into computers. In one case, a woman was stalked by a prisoner because of the 25 pages of personal data collected by Metromail. She later received mail from a convicted rapist and burglar who knew everything about her (EPIC). If the your health insurance provider has the ability to screen what type of foods you purchase, they can then start to profile and decide which health care plans they would offer based upon your life style. Without encryption your personal banking information would be open to anyone that wants to assess your financial status.

DMCA

President Clinton signed digital Millennium Copyright Act or DMCA into law on October 28, 1998. In July 17, 2001 after a presentation at DefCon in Las Vegas, Dmitry Sklyarov was the first person arrested and charged under the DMCA. Dmitry had just finished a presentation on the strengths and weaknesses the encryption of Adobe's E-Books. At the behest of Adobe, the FBI arrested Dmitry and placed him in jail without bail for two weeks. Dmitry's has been release on 50,000 bail and not until December 2001 was allowed to return home to Russia. He is waiting his court date in late 2002. Dmitry is a Russian computer security researcher and the copyright holder of the Advanced eBook Processor (AEBPR). According to the company's website, the software permits eBook owners to translate from Adobe's secure eBook format into the more common Portable Document Format. The software only works on legitimately purchased eBook's and has been used, for example, by blind people to read otherwise-inaccessible PDF user's manuals, and by people who want to move an eBook from one computer to another (Freesklyarov). Dmitry is charged with being in violation of Title 17 United States Code, Section(s) 1201(b)(1)(A) and 18 U.S.C. Sec.2 which states:

> (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that -
>
> (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;
>
> (2) As used in this subsection -
>
> (A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure.

So was Dmitry wrong for both developing a program and presenting this program at a conference? According to Russian law, it is legal to own a copy of a program if obtained legally. So under Russian law, Sklyarav was not acting unlawfully by creating a program that creates lawful back-ups of programs. In this case the FBI asserts through the DMCA that the law can be broken even if the violation is done outside US borders. Section 15(2) of the Russian `Rights protection of computer software and databases` Act states that the person who legally owns a copy of a computer program or database has the right, without the consent of the copyright owner and without payment of an extra fee, to carry out the following actions:

1. To carry out adaptation of the computer program or a database;

2. To make a copy of the computer program or a database provided that this copy of the program is intended only for the archival purposes or (if the original computer program or database is lost, destroyed or became unsuitable for use) for replacement of legally acquired copy (Freesklyarov).

The reason the DMCA is a violation of our privacy is because it makes research techniques like reverse engineering a crime by stating the research promotes circumvention technology. Ed Felton's case on the Secure Digital Music Initiative or SMDI is an example of how research can turn into a criminal case. Ed Felton is an Associate Professor in the Computer Science Department of Princeton University. Felton was took part in a public challenge presented by SDMI to break the new watermark technologies that are used for copyrighting music. Ed Felton was able to successfully crack the encryption behind the watermark technology, but instead of collecting the monetary award, Ed decided to publish a paper based upon his research into cracking the watermark technology. SDMI and the Recording Industry Association of America or RIAA promptly threatened to sue him under the circumvention technology terms under the DCMA if he went public with his findings. Felton decided against presenting the material for fear of litigation, but later decided to challenge SDMI and RIAA. Later SDMI and RIAA stated that they never intended to charge Felton with the DCMA. Felton then decided to file suit against SDMI and RIAA, but he suit was later thrown out because no formal charges were filed against Felton. On August 15, 2001, Felton publishes his paper on breaking the watermark technology and no litigation has ensued to date.

Philip Zimmerman and PGP

Philip Zimmerman is the developer of Pretty Good Privacy also known as PGP that pre-encrypts your messages before sending tem through Clipper-equipped devices (Godwin). Back in 1992, Zimmermann – Disturbed by indications that the U.S. government might try to restrict individuals' access to encryption technology outright – took several months off from his consulting job and wrote the first version of PGP (Godwin). Zimmerman stated "I wanted people to have access to this technology in the United States before the crackdown occurred" (Godwin). Upon

arriving to America after a trip to Eastern Europe, Phillip Zimmermann was detained by Dulles Airport customs agents and interrogated about why PGP had appeared in Eastern bloc countries. Zimmermann was charged with the dissemination of PGP outside the Unites States, but all charges were later dropped. He was alleged to have violated the State Department's International Traffic in Arms regulations (Gutter). In 1996 the Unites States Attorney's Office in San Francisco formally ceased its investigation of Zimmermann (Godwin). This was after Zimmermann appeared before a House committee and being detained on multiple occasions. Zimmermann proves that encryption can be created within domestic borders, although the amount of persecution that Phillip underwent is clearly a deterrent to produce further encryption. Since this information cannot be traded across the borders of the United States, then all of the research and development must also be original. This also stagnates the creative process of engineering new encryption.

Clipper Chip

Orson Welles stated "Only in a police state is the job of a policeman easy." (Godwin). The President Clinton administration proposed an encryption device by the name the Clipper Chip. This chip encrypts data sent between two devices and cannot be decoded by outside parties except for the government. The administration recommended implanting this chip in all communications devices. This would allow the government to easily eavesdrop on anything from email correspondences to telephone calls. The Clipper chip send a stream of data called a Law Enforcement Access Field (LEAF) and must negotiate the transaction before a session can be established. Once the connection is established the two devices can communicate on a secure channel. The key to the Clipper Chip is that the government retains the master key and has the ability to open any channel without a warrant if deemed necessary. Conceivably the government would hold the keys to all sensitive information which could include industry trade secrets. This would allow the policing agencies the ability to read trade secrets from all domestic companies that arguably leverages true capitalism in favor of a ruling class. The American Civil Liberties Union is against the Clipper Chip represents the invasion of privacy and states this is exactly reason why we broke from England over 200 years ago. The government ultimately decided that the Clipper Chip would be offered voluntarily and not dictated as the standard and allows citizens the freedom of choose. Because companies like Microsoft and Novell and Lotus aren't allowed to sell encryption to the world market, they are unlikely to develop strong, easy-to-use alternatives to Clipper. This means that unless you develop your own encryption package, then your options are limited to devices like the Clipper Chip (Godwin).

Steganography

One of the technologies used to ensure that messages are kept private is called steganography. Steganography is the art of writing in cipher, or in characters, which are not intelligible except to persons who have the key (Dictionary). Steganography can be viewed as akin to cryptography. Cryptographic techniques

"scramble" messages so if intercepted, the messages cannot be understood. Steganography, in an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message will not (Johnson). Modern techniques of steganography involve embedding a message into a file like a jpeg or mp3 in a manner that modifies the least significant or redundant bits. This allows for the message to be woven into the file so that it will not be noticed. The person listening to the file, or looking at the picture will not be able to tell the difference between the original and the modified file. An added security feature is the ability to encrypt the message. Now even if the file is caught as a suspicious document, the encryption has to be cracked. The success of steganography lies in the secrecy of the communication. This technology also does not require expensive technology to create and deploy hidden messages. By the same token it does require enormous computing power filter and analyze all suspicious material for hidden messages.

Shortly after the attacks on September 11th, USA Today published an article stating that Osama bin Laden had used steganography to communicate with his sects. Louis Freeh said “Uncrackable encryption is allowing terrorists – Hamas, Hezbollah, al-Qaida and others – to communicate about their criminal intentions without fear of outside intrusion,” (Kelley). One of the terrorists convicted of the 1993 World Trade Center bombing used encryption to hide details of plots against 11 U.S airliners. The U.S. was able to break the encryption used by Ramzi Yousef, but took the FBI more than two years to decrypt (Kelley).

What should we do?

The question that we should ask ourselves is “What civil liberties are we willing to relinquish so that we might protect the fabric of Democracy”. If we forgo our civil liberties then are we truly free? Does the USA PATRIOT Act allow law enforcement agencies the ability to track and arrest agents of chaos, or does it allow trample the civil liberties of the persons our Constitution was written to protect? Without the ability to test a product for reliability and the DMCA placing restrictions on an individual’s ability to reverse engineer current products, we are opening ourselves to the mercy of those individual who don’t abide by the law. Should law enforcement agent be given the tools to easily decrypt private messages and collect data on those citizens to protect our nation? Does an individual “opt-in” or consent to information being collected on them by simply opening a web site? Technology has allowed us to truly become a society without limitations. It is only befitting that while we continue to embrace technology and integrate it into our existence, that we must address the misuse of said name innovations. The difference between proper use and misuse of technology is in the manner, which that technology is deployed. Law enforcement has had the most difficult time adjusting to the flourish of technology. The first steps taken towards giving law enforcement a competitive advantage was via the USA PATRIOT Act of 2001. I believe it is clear what the intentions of our nation are by the $600,000,000.00 allocation under section 103 of

the USA PATRIOT Act for the FBI's Technical Support Center. Time will only tell if we have irrevocably detached the constitutional rights we are trying so diligently to defend. I believe that we are answering today's threats with the best of intentions and will have the foresight to change course if we discover we have gone too far. I have asked myself to what lengths will we go to protect our freedom and I believe that Tom Lantos best described my sentiments in the documentary The Last Days. Tom is the only serving United States Senator who is a Holocaust survivor as of 2002. Tom was a Jew living in Hungary during World War II living while Nazi Germany was slowly placing Jews under arrest and forcing unjust standard upon them based upon their race. When Tom was asked why he didn't leave Hungary while Germany was clearly persecuting the European Jews, he answered, "There was a sort of… patriotic feeling that we Hungarians don't do things like this." I pray our nation shares does not fall victim to the same naivety.

References

Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1802(a) (1988)

Froomkin, M. A.The metaphor is the key: cryptography, the Clipper Chip, and the Constitution. URL: http://www.law.miami.edu/~froomkin/articles/clipper1.htm(October 7, 2002).

Godwin, M. Cyber rights: defending free speech in the digital age. New York, NY: Random House.(1998).

Goode, S.The right to privacy. New York: Franklin Watts (1983).

Gutter, R. A Survey of Recent Threats to Privacy Rights. URL: http://rr.sans.org/privacy/survey.php (October 7, 2002).

Holmes, B. The Third Amendment. Englewood Cliffs, N.J.: Gallin House Press, Inc. (1991)..

Kelly, Jack, "Terror groups hide behind Web encryption", USA Today. (February 2, 2001).

Mission Statement. URL: http://www.nsa.gov/about_nsa/mission.html.(2002, March 7).

Moll, J. (Director).The Last Days. [Video]. Shoah Foundation. (1998)

Peha, J. Encryption policy issue. URL: http://www.ece.cmu.edu/~peha/encrypt.pdf. . (1998, October).

Background on the case of Dmitry Sklyarov and the DMCA. URL:http://www.freesklyarov.org/background/index.html (October 7, 2002).

Sondreal, B. Powered by Carnivore: Updated Legal Issues and the USA Patriot Act. URL: http://www.giac.org/practical/Brian_Sondreal_GSEC.doc. (2002, March).

The History Channel (Documentary). (2001). The Code Breakers.

Title 18 of the U.S. Code § 2518(7) (1988). Way, P. (1977). Codes and ciphers. United Kingdom: Aldus Books Limited.