

Encryption and Rights of Liberty

Paul Ingemi

25 October 2004

Abstract

Advancements in cryptographic technology from World War II to the present day have consistently outpaced the ability of society to form a well-accepted democratic mechanism for governing the technology. This failure has led to dispute on the proper use of cryptography. This paper examines first the historical and social dimensions of this divide between society and cryptography, then analyzes the liberal political framework for proper use of this technology, and lastly proposes obligations cypherpunks have to educate the public concerning computer technologies and individual freedoms.

Contents

1	Cryptography Issues in the Modern World	3
1.1	Rise of Private Cryptosystems	3
1.2	Stakeholders	4
1.3	Information	5
1.4	Government Controls on Information	7
1.5	Code breaking	8
1.6	Freedom of Speech/Academic Freedoms	9

2	Merchants on an Army Trail	10
2.1	Another Great War	10
2.2	A Standard	11
2.3	Trading Blood and Wine	12
2.4	Clinton Administration	13
2.5	Phil Zimmerman	14
2.6	DVD John	15
2.7	Sklyarov	16
2.8	VOIP	17
3	The Rights of Liberty	17
3.1	Nobody’s Business but Yours	18
3.2	Liberalism and You	20
3.3	Conclusion	22

1 Cryptography Issues in the Modern World

“Gentlemen do not read each other’s mail.”

– Henry Lewis Stimson

"You have zero privacy anyway, get over it."

– Scott McNealy, CEO Sun Microsystems

In most societies, there is an ever-constant struggle between the expanding capabilities created by new and improved technologies and the force of law that restrains, regulates, and makes such advancements safe for society as a whole. Cryptography is an ancient technology that has matured rapidly in the last twenty years such that, despite its age, it is increasingly becoming a fault line for the schism between the individual need to protect one’s privacy and the state’s need to protect both individuals and themselves. The capabilities of today’s cryptosystems present a new source of power for both governments and individuals: individuals have enhanced powers to keep secrets hidden from the government, and the state has new powers to keep their secrets safe from the individual. The power of modern encryption creates a struggle where both the individual and the state is working to limit the technological power of the other.

1.1 Rise of Private Cryptosystems

The cryptosystems of the past can be categorized into two types: codes and ciphers. Although semantically identical words in modern parlance, codes refer to languages and ciphers refer to secret methods of writing. For instance, a code may be an agreement that “mother, how are you” means “the jig is up!”, while a cipher may involve changing A to B, B to C, and so on. For example, “Jung qb lbh uvqr?” is decoded to “What do you hide?” by advancing each letter 13 times. Both of these forms of message obfuscation can potentially be unbreakable, however almost all practical implementations of contemporary cryptography are possible to break.

Precipitating the 1980s rise of computers and information technology to prominence, ciphers in the 1940s became unconstrained by traditional human limitations. Advancements in ciphers

created cipher machines that seemed unbreakable. The German *Enigma* and the Japanese *Purple* are popular examples of this trend toward mechanical cipher devices that seemed flawless, but ultimately were not. While *Enigma* was based on a commercial product, the realm of cryptography remained relatively isolated to large, special interest groups. The main players in this conflict between the power of secret messages and that of reading them were constrained to the governments of the world. This would soon change.

In 1991, Phil Zimmerman released a program called *Pretty Good Privacy*[12]. PGP is a free cryptosystem designed for public use. Despite this, it was and still is fairly complicated for the average person, and so the public has not directly benefit from the release of this program. The indirect benefit, however, is that the release of PGP marked the opening of the floodgates of public use of cryptosystems.

As a result, today, securely ordering goods over the Internet is common; so is protected passwords and files. Consumer cell phones have gone from unencrypted analog transmissions to encrypted digital signals. Encryption today has become pervasive, however in most cases it benefits entities other than the general public, such as private corporations. Because most uses of encryption by the public today primarily benefit business and government interests, the main stakeholders in the control of private cryptosystems are still a vocal minority and not the public at large.

1.2 Stakeholders

There are three main stakeholders to consider: citizens, criminals, and governments. Citizens all have their own reasons for using cryptography, however they can be generally categorized as needing protection from lawbreakers and/or needing protection from government. Citizens may want to keep their credit card information secure from crackers who might intercept such data or keep their personal dealings hidden from prying eyes in the family, or they may cross the line between citizen and criminal and keep incriminating information hidden from the government.

Governments generally have the job of protecting citizens and protecting themselves. This entails the responsibility to diligently monitor for threats to either. Such monitoring necessarily

involves either invading the privacy or limiting the freedom of individuals. But without privacy, there is no freedom, and without freedom there is no privacy. Therefore a government's best interest in cryptography tends to be inherently opposed to that of a democratic society that believes in rights of privacy.

Criminals, of course, need cryptography to protect themselves from capture and punishment. Citizens are typically threatened by criminal behavior, and therefore it is in citizens' best interest to curtail the freedom of a criminal. Similarly, criminals can threaten the sovereignty of the state, and so the state must seek to limit the freedom of criminals. Lastly, criminal activity can threaten other criminals, and so criminals even seek protection from each other. Cryptography provides that protection by anonymizing a criminal's identity and hiding a criminal's information.

1.3 Information

Some of the many types of information secured by cryptography are copyrighted data, business data, anonymous cash, espionage, illegal data, anonymous data, age or location controlled data, voice data, and illegal markets[1]. This list is not exhaustive, however it provides a good starting point to begin discussion. Early pioneers of public cryptosystems predicted legal problems developing in these areas and without fail each area has been challenged by those who want public use of them controlled.

In the area of copyrighted information, as in most areas, cryptography is a two-sided sword. Content manufactures, or companies whose products are intangible intellectual creations like movies and books, control their content through copyright and are increasingly looking toward encryption to control how their works are used. In theory, any cryptosystem designed to deliver content to consumers while simultaneously protecting it from those consumers is doomed to fail, because at some point the content needs to be decrypted to be viewable. In practice it appears to work quite well, because the effort required to find a way to get at the decrypted content provides a high bar for entry. The flip side of the blade, however, is the use of cryptosystems to illegally traffic these copyright-protected works and anonymize the distribution such that the copyright owner's control

is weakened.

In the area of business data, cryptosystems can protect businesses from criminal mischief as well as protect such businesses from government intrusion. For instance, hospital and health care records are held to extremely high standards of protection against unauthorized disclosure. Encrypted communication lines are extremely important tools in the arsenal of hospitals, when used to get medical information where it needs to go quickly without compromising its security. On the other hand, businesses can use such secure lines for illegal activities such as to coordinate prices, trade insider information, or double book and keep the second book private.

Anonymous currency, or money that is not easily traceable, is an important form of information for those who want to escape government interference. The idea is that through cryptosystems, a trusted authority can digitally sign bank notes to give them value as money[2]. Although similar to other non-official tender, this has the benefit of being easy to create, extremely difficult to counterfeit, liquid, and not linked to an identity. It can be used to facilitate money laundering and tax evasion.

Espionage is the bane of governments, corporations, and individuals. Spy-craft necessitates the need for anonymity and secrecy. Keeping secrets is inherent to the nature of this business and not much more needs to be said about it.

Some forms of information, with or without encryption, can be in itself illegal. This includes obvious examples such as sexually explicit depictions of underage children, but it can also include computer programs with the potential to view DVDs. While programmers contend that writing in a language computers understand exercises free speech and should be protected as such, the US courts have disagreed on how far that protection extends, leading to programs such as a DVD reader for Linux to be declared illegal[14]. Creators and consumers of this type of information may use cryptosystems to protect themselves from those who control this type of information.

Anonymous information is often of general importance. For instance, e-mails with no identifiable sender can be sent through a re-mailer network. These networks consist of nodes that know only enough about the message to send it on to the next node or to the final destination. This

is typically done with a technique called onion routing, where the message is encrypted and the instructions for each node that passes the message is appended to the message and encrypted again such that the node can decrypt it. Thus, each messenger peels off a layer of the onion by decrypting it with the messenger's private key and reveals only enough information to pass the message on to the next node. Other anonymous networks are more sophisticated, such as *freenet*, which affords completely anonymous publishing of information into the system.

Voice information, such as digital cell phone calls, are encrypted. This allows users to converse with relative certainty that their conversations are not being overheard. Other methods of conversing using voice include programs that allow you to talk over the Internet. Typically that technology falls under the umbrella VOIP, or *Voice Over Internet Protocol*. The main threat to the security of VOIP is the government attempting to regulate these programs much like they regulate normal phone carriers: by taxing them and requiring wiretap ability[1]. The government contends that this is merely a logical extension of the already existing ability to tap cell phones and land lines. Privacy advocates counter with the assertion that originally the government could not listen in on any conversations at all before there were telephones, and the logical extension of that is there should be no government capacity for eavesdropping at all.

Illegal markets are another area where cryptography can play a protective role. Cryptosystems can hinder government interference in such markets. These are markets on illegal information, i.e., "futures markets" on the lifespans of undesirable people, otherwise known as hiring an assassin, and other markets involving criminal intent[2].

1.4 Government Controls on Information

With the potential for unrestricted information flow protected by cryptography established, the government has no choice but to act. The government has a few tools for containment: export restrictions, common carrier laws, data retention laws, and court compelled testimony and evidence. These provide a strong non-technological method of breaking today's public cryptosystems that experts like to classify as "rubber hose cryptography." [3] So called, because a rubber hose can be

a brutal tool to break people behind the system without needing to break the system itself.

Curiously, cryptosystems have been classified as weapons, and are subject to ITAR (*International Trafficking in Arms Regulations*)[8]. This fact has led to the production of t-shirts with cryptosystems written on them, creating the ironic realization that such t-shirts are in fact considered weapons. Despite attempts to show the ridiculous nature of such a classification, these restrictions have proved an effective tool. By branding cryptosystems as weapons, the US government controls the strength of exported cryptosystems. As a consequence, rather than develop multiple versions of a product, companies often develop products with only weak encryption that can be marketed both inside and outside the US. Some companies with large resources such as IBM attempt to sidestep the issue by developing the cryptographic products outside the US and then importing rather than exporting it.

Another set of laws is the common carrier laws. These laws protect “common carriers”, or services that must accept all customers and cannot violate the customer’s privacy, from liability for the customer’s actions[4, Common Carrier]. Examples of common carriers include the mail system and the phone system. These laws would help anonymous cryptosystems, which similarly protect privacy and fail to discriminate their customers, however the prevailing notion is that in exchange for common carrier privileges, the service must also help the government. For instance, in the case of phone services, this help comes in the form of wiretapping ability. In the case of Internet Service Providers, detailed logs are required for immunity from liability.

1.5 Code breaking

Code breaking is an integral part of the creation of cryptosystems. The security of today’s cryptosystems comes not from secrecy about how they work, but peer review to weed out the ones that may break easily. That means those who produce cryptosystems also try to crack them. Lately, however, the government has taken a dim view on those who break cryptosystems.

Laws against breaking the encryption protecting cable and satellite TV have been in the books for a while. Recently the *Digital Millennium Copyright Act* (DMCA) was passed making it a crime

to break codes protecting copyrighted content[4, DMCA]. Essentially this creates a catch-22: even though you may have the legal right to use a copyrighted work, you are not allowed to remove the protection that is preventing you from using it. Two big cases brought this to the attention of programmers everywhere.

The first public case was against the *2600* magazine for publishing the source code to a utility called *decss*, which decrypts DVDs into a form where they can be played under Linux. A Linux user who owned a DVD and wanted to play their DVD would use this utility, however because playing a DVD requires decrypting it first, *decss* ran afoul of the DMCA. *2600* was prohibited from publishing the source code or information about where to find the source code[14].

The second case was against a Russian programmer named Dmitri Sklyarov, who wrote a program to convert adobe ebooks into other file formats. While legal in Russia, the US considers this a crime because converting the ebook requires first decrypting it. When Dmitri flew to the US to attend a programmer conference, Adobe noticed his name and had the US arrest him. Thankfully, he was released back to his wife and kids under the condition that he would testify against his employer[15].

1.6 Freedom of Speech/Academic Freedoms

Freedom of speech and academic freedom issues have been discussed above in several places. Typically these issues fall into two categories: freedom of speech protected by cryptosystems, and freedom of speech about cryptosystems. The former has been well covered, but the latter deserves further scrutiny. Essentially at issue is whether writing in a form that machines can read is free speech or unprotected speech. Judges, under the theory that programs act as mechanical devices, sometimes subscribe to the theory that programs have unprotected speech elements to them. Programmers usually subscribe to the theory that computer languages are languages like any other, and their choice to express themselves in that language should not be an impediment to their freedom of speech.

2 Merchants on an Army Trail

“Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders.”

– Ronald Reagan

The transition of cryptography from pen and paper tricks and mathematical amusements to long complicated calculations and serious business was catalyzed by war. Just as the crusades, marked by bloody battles between the Muslim-lands and Christendom, ultimately led to the establishment of trade routes between the two great regions, so too does World War II kick-start the fast evolution of the cryptosystems that enabled global internet trade.

2.1 Another Great War

In the art of warfare, military intelligence is as important as military fire power. This is because application of force requires information on how it may be used effectively for the given situation. According to Kahn, in August 1914, the German naval codebook fell into the hands of England by way of Russian spies leading to the dramatic reduction in the effectiveness of the German Army in the North Sea[3, 972]. When the Germans discovered that the security of their system had been compromised, they took steps away from codes and codebooks toward a mechanical cipher system. This system would be known as *Enigma*.

Enigma is a *polyalphabetic substitution cipher*, or a cipher where “the plain-text letters are enciphered differently depending upon their placement in the text.”[5]. The mapping of the plain-text alphabet to the cipher-text alphabet is determined by a plugboard and the electrical connections between a series of rotors. For each letter encoded, the “fast” rotor advances one position. For each full rotation of a given rotor, the next rotor advances one position. With this setup, the alphabetic substitution changes on every letter enciphered. Furthermore, the encoding and decoding key is the initial position of the rotors. This is a mechanical codebook that, when leaked, does not compromise the security of the system. The adversary still needs the initial rotor setup.

... or so they thought.

“Franciszek Pokorny [of Poland] recognized ... what was needed to solve them [mechanized cryptosystems] was not classical scholars and philologists but mathematicians.” [3] So therefore he recruits mathematicians with cryptographic backgrounds who, through ineptitude on the part of the cryptosystem users, leaked information about *Enigma* and key mathematical insights, developed an attack that could break the security of the system. The Germans upgraded the strength of their *Enigma* machines by adding additional rotors, soon out-pacing the ability of the Polish mathematicians to solve for the initial rotor configuration. The information on *Enigma* as well as the code-breaking techniques and machines were passed on to France and England, with the English ultimately taking the final steps to break the full five rotor system within reasonable time constraints.

Even though World War II had come to a conclusion, the secrecy surrounding breaking enigma survived for another thirty years, until 1974, when England approved release of the information in the form of a book titled, *The Ultra Secret*[3]. According to Kahn, this secrecy served the purpose of protecting the Enigma user-base, such as former colonies, which had been provided with Enigma machines to secure their communications. The more cynical view is that the England benefited from the continued use of a broken cryptosystem.

2.2 A Standard

On the 15th of May in 1973, the US government put out a request for proposals for a new standard... a *Data Encryption Standard* (DES)[3]. Even before England’s disclosure of cracking *Enigma*, the US Government realized that a strong encryption system was in the best interest of US businesses and possibly citizens and the government itself. Having it public allowed for the standard to be scrutinized for security and led to commoditized hardware implementations. IBM proposed a scheme known as *Lucifer* that was accepted after modification by the government. *Lucifer* gained a new name: DES[4, DES].

Because the government, particularly the NSA, was involved in improving IBM’s proposed

scheme, some people theorized that DES had been weakened [4, DES]. It is still up for debate; however we do know that the changes hardened DES against differential cryptanalysis, a publicly unknown attack that the NSA convinced IBM to keep secret. On the flip side, in 1998 the Electronic Freedom Foundation demonstrated a \$250,000 machine named *Deep Crack* that is able to crack DES in about a day. Earlier efforts had been successful in cracking DES with networks of computers working together, however *Deep Crack* demonstrates that deciphering DES is easily within the power of any small country, and the government may already have such machines.

2.3 Trading Blood and Wine

Nation States clearly benefit from the popular use of cryptography to protect data; however any government sponsored use of the technology is also a blow to their ability to monitor the uses of cryptography that the government does not endorse. This is because most uses of cryptography, while encrypting information, also leak information. This may be sender and recipient information, however more fundamentally, the use of cryptography is in and of itself an indicator of the nature of the information. What hurts governmental authority is that as cryptography becomes more and more prevalent, the usefulness of this relationship decreases.

In 1993, the US government announced a voluntary standard for encryption known as *Clipper* [7]. This standard involved a secret encryption algorithm, SKIPJACK, implemented by tamper-proof hardware. This standard also provides for a key escrow. A key escrow maintains a copy of the encryption key in a secure manner, only revealing the key through a court order or as otherwise required by law. From the standpoint of the US government, this satisfies the needs of those who would use encryption on the right side of the law, while seriously hurting those who would misuse it. Adoption of the scheme met huge resistance along three lines: First, the secrecy of the scheme made potential users wary about the strength of its encryption. Publicly used cryptosystems are generally not secret, and peer review of the encryption allows for some degree of confidence in the system. While the US government did have outside experts review the system, its private nature makes confidence in it that much less. Second, the key escrow itself could be compromised. It is a

single point of failure for the system, because once it is compromised, every message protected by SKIPJACK would no longer be protected. Lastly, some people simply prefer that the government remains locked out of their information [6]. There were further concerns that the “voluntary” status of Clipper could evolve to what voluntary payment of taxes is now.

Upon declassification in 1998, SKIPJACK was revealed to be a highly fragile system, in that it withstands cryptanalysis however any small change to it yields a significantly weaker cipher. Within a day, attacks were formulated for reduced round versions of SKIPJACK, and later ones could handle up to 31 of SKIPJACK’s 32 rounds[4, SKIPJACK]. While these attacks do not work against the full SKIPJACK, they lead to strong doubts regarding the overall security of the scheme.

For comparison, England takes a more practical tact on government access to keys. Simply put, if asked, an English subject is compelled to provide his keys or face two years in jail.

2.4 Clinton Administration

The key escrow does not end with the failure of Clipper, and is given new life under the October 1, 1996 Key Recovery Plan of the Clinton administration. The plan loosens cryptographic export restrictions present in the International Traffic in Arms Regulation (ITAR). According to ITAR, cryptography falls under Category XIII:

- (1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems[8, Category XIII b1]

Against a backdrop of a strong computer industry demanding reforms to this law, President Clinton proposed reduced restrictions for those products that plan to include key escrow over a two year period, with non-escrow systems prohibited when the two years are up[9]. In other words, the Clinton administration “favors strong cryptography, but not too strong.” [10] These measures to reintroduce key escrow met the same response as Clipper and had the Clinton administration not relaxed restrictions on strong cryptography without escrow, the senate would have done it for them.

2.5 Phil Zimmerman

When Phil Zimmerman, an MIT professor, released Pretty Good Privacy in 1991, he was racing against time to preempt government regulations that might have made strong cryptography illegal.

PGP was developed under difficult conditions, with no funding, in a race against time in 1991 to get it out before it became illegal to publish software of this type. Senate Bill 266, the 1991 anti- crime bill, had a measure buried in it that foretold the shape of things to come.[11, preface]

The bill in question, if it had become law, would have required “back doors” to be implemented within secure communication equipment. This would give the government the ability to read communication secured with these devices, against the wishes of people like Phil, who claim “Its personal, its private, and its nobody’s business but yours.”

After the release of version 1.0, PGP was distributed electronically and leaked outside of the US. The first group to complain was RSA Data Security which has a patent on some of the technology in PGP. The patent issues with RSA Data Security were resolved, however the government had become interested and started a three year investigation of Phil Zimmerman on allegations that he distributed the source code outside the US in violation of ITAR[12].

After three years, the investigation was closed. The defense attorney’s take on the matter was that they chose not to prosecute because they had not found proof that Mr. Zimmerman did anything wrong, because they feared the export laws might be overturned, or both. Despite not prosecuting Phil, exporting cryptography will be considered serious business until the year 2000 when export controls on high cryptography are loosened.

Presently, the key encryption algorithm used by PGP (pun not intended) has taken on a new role in ridiculing ITAR, with t-shirts printed with:

```
#!/bin/Perl -sp0777i<X+d*1MLa^*1N%0]dsXx++1M1N/dsM0<j]dsj
$/=unpack('H*',$_);$_='echo 16dio\U$k"SK$/SM$n\Esn0p[1N*1
1K[d2%Sa2/d0$^Ixp"|dc`s/\W//g;$_=pack('H*',/(.)*$/)
[Author Unknown]
```

This is completely functional RSA encryption in three lines of Perl code.

2.6 DVD John

In 1996, a new dimension to legal use of cryptosystems entered the fray. The World Intellectual Property Organization, which seeks to harmonize the protection of intellectual property worldwide, developed the WIPO Copyright Treaty. Article 12 of the treaty prevents circumvention of technological measures for the protection of works. Technological measures almost invariably refer to cryptosystems used to protect said works. Article 12 therefore becomes a means to control such cryptosystems in countries that adopt laws pursuant to the agreement[4, WIPO Copyright Treaty].

The US upgrade of its copyright laws was titled the Digital Millennium Copyright Act (DMCA), and included provisions to satisfy article 12. Furthermore, the US's stance on what article 12 means in practice is that the copyright holder for a work that is encrypted is the only person who can create or give permission for creation of the associated decoder. What this means for US citizens is that should you own a DVD and require a single picture from the movie, as you are allowed under fair-use doctrine for certain purposes, you may only do so if the DVD decoders support extracting a single image. You may not build your own decoder to extract a single image because it would be construed as circumventing a technological measure for the protection of works.

In 1999 these laws had not been exercised and this particular interpretation of the law had not yet been established. This was the year a Norwegian, Jon Johansen, released a program called *decss*. The *decss* program was an unapproved DVD decoder that had been developed by reverse engineering other authorized DVD decoders. With *decss*, exercising fair-use to extract a single frame of a DVD become possible. So did watching DVDs on computer platforms that otherwise wouldn't support it. Because it potentially runs afoul of the law, the Norwegian white-collar crime

prosecution organization, Okokrim, tried twice to prosecute Jon for computer crime charges however both attempts failed. The Norwegian interpretation of Article 12 allowed for the creation of unauthorized decoders.

In the US, a magazine called *2600*, after the 2600Hz tone used to control phone trunks, distributed the code for *decss*. The Motion Picture Association of America (MPAA) filed an injunction to prevent *2600* from further distributing the code. The surprising outcome of the injunction was that not only is *2600* not allowed to distribute the code, but they are also not allowed to link to the code. This judgment was surprising because it seemingly violates the freedom of speech; however, the judge makes a razor fine distinction to separate free speech this unprotected speech: links that allow a computer to automatically download the code when clicked have a non-speech component to them that allows them to be barred, whereas a link that doesn't do anything when clicked would not be restricted[14]. The author of this paper wonders whether this decision would extend beyond computer code to English once computers can understand and perform instructions in both equally well. One Slashdot reader acutely pointed out: "Why can't they [WIPO] harmonize the laws to be *less* restrictive?"

2.7 Sklyarov

The reach of the DMCA would appear to stretch beyond merely the borders of countries complying with the WIPO agreement. A Russian company called Elcomsoft produced a program that translates Adobe eBooks to a more common PDF format, for use in a broader range of devices and for a broader range of purposes. The programmer who wrote it, Dmitri Sklyarov, planned to go to the US to speak at a conference. Adobe noticed his presence as a speaker and tipped off the FBI, and so Dmitri was arrested upon entrance to the US. After a large backlash, Adobe dropped charges, however the US prosecuting attorney pressed on charging Dmitri with violating the US DMCA laws despite being in Russia and not violating the Russian copyright laws[15]. Although Dmitri was freed in exchange for testimony against his employer, this act by the US has had a chilling effect on scientists and programmers. Many scientists and programmers are now wary about

entering the US for fear of reprisal should the government dislike their research or other activities.

2.8 VOIP

Meanwhile, the current issue being hashed out now, today, is the privacy of voice communication over systems other than *Plain Old Telephone Systems* (POTS). The government would like to extend its control of such communication over any medium for purposes of taxation and wiretapping. Currently the government is classifying businesses that provide means of doing voice communication over the Internet as “telephone companies” and requiring them to uphold the same standard of wiretapping as is provided by conventional phone companies. To meet these demands, Internet telephone companies need to either provide no encryption, encryption using their keys, or key escrow. This is an issue because voice communications over the Internet are normally established between sender and caller with only the Internet rather than the phone company acting as the intermediary. Thus, key escrow and no encryption would appear to be the only ways to meet these demands, and both means are disagreeable to many people including the Internet phone companies.

3 The Rights of Liberty

“We have to destroy Arkology to save it. I know it sounds bad.”

– Dylan Hunt, *Andromeda*

“If it doesn’t apply to everyone, it means NOTHING.”

– Captain Kirk, *Star Trek*

After examining current issues between individual and state interests in cryptography, and their historical development, the question remains: what is the right approach to the regulation of such technology? What is the right thing to do? How can the average person ensure his or her own personal liberty through the use of cryptography? The nation-state’s attempting understandably to

secure national sovereignty may be necessary, but may lead to encroachments upon the rights of citizens. How may both national and individual interests be served?

3.1 Nobody's Business but Yours

One common theme among proponents of unlimited strong encryption is that encryption allows citizens to actively and vigilantly enjoy their right to privacy. The notion of privacy in that case includes the ability to suppress release of information in your possession that you do not want others to have. Believers in strong cryptography will necessarily see the right to privacy in terms of something cryptography can protect. Therefore, this view of privacy is a natural consequence of the belief of many of those who hold it. This ability to suppress other's use of what you possess would be a property right. However, the right to privacy, at least in the US, constitutionally rests upon a different basis.

Before December of 1890 when justices Warren and Brandice[4, Right to Privacy] published in the *Harvard Law Review* an analysis of the basis for the right to privacy, a person's privacy was mainly protected through the use of property law, contract law, as well as libel and slander laws. Property law gave people the ability to exclude others from using private information contained within a piece of property. For instance, a diary may contain sensitive information. Anyone who then steals the diary and learns about that private information has committed a crime in doing so. Contract law can be used to show trust relationships through written or implicit contracts; and those trusts can protect private information from being improperly used. For instance, a person visiting a bathhouse might reasonably expect the business not to take clandestine photos while the patrons are bathing. The business contract comes with implied trust relationships like these. If the bathhouse were to engage in such unethical acts that violate a trust relationship, they could be held liable for contract violation. And lastly, libel and slander laws allow legal redress for publication of untrue "facts". While arguably, such falsehoods are not a direct violation of one's privacy, they may put public scrutiny on the individual. The result of such public scrutiny is a net loss of privacy, because it may violate their desire to be left alone.

Warren and Brandice pointed out that the right to privacy, if it exists, should cover situations that property law, contract law, and libel/slander laws do not protect. For instance, noting the spread of gossip, Warren and Brandice posited that a person's reputation could be irreparably harmed by gossip. The recent (for the time) developments in cameras allowed compromising information to be compiled without the active participation of the person. For instance, a passive observer could photograph someone's daily life. This form of intrusion rules out property and contract law protection, and further, the damage is irrespective of the truth of the gossip, ruling out libel and slander as viable protection. Warren and Brandice make the prescient conclusion that any such privacy right has to be broader than the established laws, and essentially innate to the person: "the right to one's personality" [16].

What Warren and Brandice refer to as "the right to one's personality" is a liberal concept whereby people have the right to be reasonably free from coercion by others. That is to say, other people should not forcibly influence their personality and sense of who they are. Without privacy, people would need to consider how their otherwise private actions would reflect publicly upon them, allowing external forces to dictate personality through all aspects of life. Warren and Brandice saw this as wrong.

Since publication of "Right to Privacy" in the *Harvard Law Review*, the principles of privacy have been slowly worked out and ossified. It is now a well-known concept framed in the Universal Declaration of Human Rights:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. (Article 12)

However, the meaning of privacy and honor, as understood in Article 12, has taken new forms since the 1890s. Everyone has a right to privacy, *but it seems that some people* have more right to privacy than others. In the US and many other countries, people deemed to have celebrity status do not have as much protection from gossip as the average person. For example, a movie star may be considered to be in the public light, and benefits from such publicity, and thus does not

enjoy privacy protection as comprehensive as the average citizen's protection. Reporters regularly follow the public and probe into the private life of these highly visible individuals. Indeed in these times, gossip is not seen as the evil that Warren and Brandice painted it as. Moreover, the attitude toward a right to privacy is different in the US and European nations: the US tends to favor freedom of speech over the right to privacy, and European nations take the opposite stance. For example, newspapers in the US regularly publish names of arrested individuals and suspects because the US values the freedom of the press over the privacy of those individuals. On the other hand, newspapers in England do not identify suspects because European countries tend to value the privacy of those suspects over the freedom of the press.

So while a right to privacy is now understood to be broader than a property right, it does not necessarily function as a property right. While encryption can protect privacy and property, its protection extends beyond what the legal idea of privacy entails. This is because it protects your property against the government, even in instances where they do not legally consider your property to be private from them, such as when they have a search warrant. It acts as an absolute guard of unpublished intellectual property. This protects your "right to one's personality" because the privacy of your intellectual efforts cannot be breached by even the state. This may help explain the Clinton administration's feelings on key escrow systems: it protects your privacy under their definition of what privacy entails. It also explains why other people were adamantly opposed to such a proposal: their ideas of privacy are much broader and more absolute than the government's.

3.2 Liberalism and You

Warren and Brandice were classic liberal jurists. In the context of cryptography, liberalism lies on three central supports: personal liberty, social liberty, and international liberty[17]. These liberties construct a framework for how people can expect to be treated by their government and peers. However, this framework is not unambiguous.

The first right, that of personal liberty, is a right to be "dealt with in accordance with the law." [17]To a liberal, the law is your protection against tyranny as well as anarchy. It is a solid grounding

to stand on that can be reasonably expected not to move under one's feet. It is necessary to have a rule of law that applies equally to everyone, because otherwise people will not be ruled by law but by other people, and that is defined to be the opposite of liberty.

As Warren and Brandice stated in *The Right to Privacy*[16], this applies directly to the notion of privacy. Without privacy, people have no “freedom from inquisition into opinions that a man forms in his own mind – the inner citadel where, if anywhere, the individual must rule.” [17] Cryptography gives people a form of protection for their opinions; however to what extent liberalism protects these opinions outside of the realm of thoughts is debatable. To what extent this right even exist is also debatable given the use of lie detector tests, which are compulsory for some criminals and required for some jobs. Perhaps the right to sovereignty of your own thoughts, free from the “inquisition” of other men, does not exist. Perhaps it should.

Social liberty is the second important liberal right. It includes freedom to pursue an occupation and freedom of association[17]. Cryptography, particularly in encrypting voice transmission and mail, helps facilitate the freedom of association, however the freedom of association in liberal parlance only extends so far as the associations themselves are liberal. This means if associations further an agenda that hurts the liberty of others, then the associations themselves are not liberal and therefore the freedom does not exist. It is difficult to distinguish between a liberal and non-liberal association protected through cryptographic means, and so whether the government has the right to control cryptography used for association despite the unknown nature of the association is debatable.

The third important liberty is international liberty. And this is where liberalism appears to require some control of cryptography. A liberal government needs to protect its citizens from encroachment by non-liberal states or groups.[17] For instance, when Adolf Hitler threatened the liberty of Europe and Russia, the potential existed for this threat to extend to the US. To preserve the liberty of Americans, the US not only helped defeat Hitler but also seeded Europe with democratic governments.

Leonard Trelawney argues that “There is a point at which speech becomes indistinguishable

from action, and free speech may mean the right to create disorder... No modern state would tolerate a form of religious worship which should include cannibalism, human sacrifice, or the burning of witches.” [17] This would appear to directly address the issue of cryptographic computer code not being protected by free speech because computer code fits the description of speech that is almost indistinguishable from action. In the RIAA vs 2600 appeals case, the judges treated the *decss* code as both a work of protected speech and something indistinguishable from action... a device for which the creator has a responsibility for. It is analogous to a Rube Goldberg machine that performs lethal injections: while it may be a work of art, it may also be an illegal device. Thus, protection on free speech does not protect program code that acts as an illegal device. This ruling is very much in accordance with liberal philosophy, however ignoring liberal rights in the process of preventing potentially non-liberal infringements on those rights seems, I would argue, to be sacrificing the liberal principles to save them.

3.3 Conclusion

There are no easy answers. There never are. The first step toward finding an appropriate compromise is to use cryptography. It's out there, for public consumption, but the public needs to use it for their private communication needs. Only when the public understands the nature of their own privacy, will they ask “Why do you need to look into my mail?” rather than “I've got nothing to hide, why should I protect my mail?” They will hopefully have a deeper appreciation for their own personal liberty, and whether government protection comes at the appropriate cost. Because until the public knows what privacy they are giving up, they will not perceive any loss. Until that happens, the few cypherpunks and human rights activists and other individuals who do use encryption need to educate and protect the liberty of the many and protect the public right to make an informed decision on how much control the government should have on their privacy.

References

- [1] Turpeinen, Marko. *Legal and Ethical Issues Related to Cryptography and Information Security*. Helsinki University of Technology. Retrieved 20 October 2004 <http://www.cs.hut.fi/~mtu/netsec/marko_1.html>
- [2] May, Timothy C. *The Cyphernomicon: Cypherpunks FAQ and More*. Retrieved 20 October 2004 <<http://www2.pro-ns.net/~crypto/chapter10.html>>
- [3] Kahn, David. *The Code-Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner. 1997.
- [4] *Wikipedia: The Free Encyclopedia*. Retrieved 20 October 2004 <<http://www.wikipedia.org>>
- [5] *Polyalphabetic Substitution*. Retrieved 20 October 2004 <<http://hem.passagen.se/tan01/poly.html>>
- [6] Begley, Sharon, Liu, Melinda. "The Code of the Future." *Newsweek* 7 June 1993.
- [7] Adam, David. "Cryptography on the Front Line." *Nature* 25 October 2001.
- [8] *International Traffic in Arms Regulations (ITAR)*. Retrieved 20 October 2004 <http://www.epic.org/crypto/export_controls/itar.html>
- [9] *Key Recovery: The White House Encryption Initiative*. Electronic Privacy Information Center. Retrieved 20 October 2004 <http://www.epic.org/crypto/key_escrow/key_recovery.html>
- [10] Lewis, Peter. *Perspective on Recent Events in Data Encryption Policy*. IEEE. Retrieved 20 October 2004 <<http://www.ieee-security.org/Cipher/ConfReports/conf-rep-Cryptopolicy.html>>
- [11] Zimmerman, Phil. *PGP Source Code and Internals*. The MIT Press: 1995.

- [12] Back, Adam. *PGP Timeline*. Retrieved 20 October 2004 <<http://www.cypherspace.org/adam/timeline/>>
- [13] Dubois, Philip. *Significant Moments in PGP's History: Zimmermann Case Dropped*. Retrieved 20 October 2004 <http://www.mit.edu/~prz/EN/news/PRZ_case_dropped.html>
- [14] *DVD Industry Takes 2600 to Court*. 2600 Magazine. Retrieved 20 October 2004 <<http://www.2600.com/news/view/article/19>>
- [15] *Free Dmitry Sklyarov*. Retrieved 20 October 2004 <<http://www.freesklyarov.org/>>
- [16] Warren, Samuel and Luis D. Brandeis. "Right to Privacy," *Harvard Law Review* 15 December 1890.
- [17] Trelawny, Leonard Hobhouse. *Liberalism*. New York: Henry Holt, 1911.