Data Encryption Software and Technical Data Controls in the United States of America

PO Box 1151
Longmont CO 80502-1151
USA

mpj@csn.org

303-447-7302

7 January 1994

1. Introduction

The current status of the regulation of encryption software in the United States of America is, at best, confusing and harmful to business. At worst, the current status is harmful to National Security and violates U. S. Constitution. I invite you to study this issue with me. I present what I perceive to be the problems and the issues that must be considered, then suggest some solutions. Even if you don’t fully agree with all of my statements, I hope that they prove helpful to your own understanding of this situation.

2. Problems with the Status Quo

I perceive several problems with the current International Traffic in Arms Regulations (ITAR) far beyond typos like the reference to §120.10(d), which doesn’t exist, in §120.10(1). These problems are severe enough that I hope that they will be rectified soon before they do even more damage. All of the problems with the ITAR mentioned here have to with encryption software, as defined in the ITAR.

2.1. Regulations Ignore Technology

The ITAR ignores the fact that software, like other technical data, can exist in a multitude of forms, many of which know no national boundaries. The ITAR ignores the fact that much of what is prohibited to be exported exists in unlimited quantities outside the USA. The ITAR hurts U. S. Business but doesn’t significantly reduce the availability of strong encryption technology outside the USA. The ITAR ignores the widespread use of purely electronic means to distribute software, such as the Internet, Computer Bulletin Board Systems (BBS), and commercial information services (such as CompuServe). The ITAR ignores the fact that shareware publishing, which is a form of Constitutionally protected publication, propagates software all over the world with no formal distribution mechanism.

2.2. Overly Broad Definition of “Encryption Software”

“Encryption software” is defined in §121.8(f) and §121.1, Category XIII(b) to include not only computer programs designed to protect the privacy of information, but all of the technical data about those programs. This naturally includes a great deal of material in any large library or book store. William B. Robinson, Director of the United States Department of State, Bureau of Politico-Military Affairs, Office of Defense Trade Controls, states in his letter to me of 30 November 1993, that “theexemptions listed in §125.4 for technical data do not apply to cryptographic software and source code.” I conclude, therefore, that the ITAR implies that the majority of the libraries and larger bookstores in the United States stock “munitions” on their shelves for anyone to read.

2.3. Overly Broad Definition of Export

§120.17 of the ITAR makes it clear that allowing a foreign person to read a book containing encryption software constitutes export. Therefore it seems possible that some perverse person might state that all of the libraries and bookstores that contain any book on cryptography must register as an exporter of munitions. This situation gets even more interesting in its electronic analogies. However, restricting domestic distribution of technology that is perfectly legal and useful within the USA just because a foreigner might see it is not only unreasonable, it could probably not stand a Constitutional challenge.

2.4. Censorship and the First Amendment

The ITAR does make some acknowledgment of the fact that not all of the publications that it calls “encryption software” need be subject to export restrictions, but doesn’t even come close to defining the difference. All it does is set forth a censorship procedure called a “Commodity Jurisdiction Procedure” (see §120.4).

From what I know of the First Amendment and Constitutional case law (I’m not a lawyer, but I took a class on the subject), the only way the Federal Government can legally take away U. S. Citizen’s rights to freedom of speech or freedom of the press is when there is a clear danger that is caused by that expression, or a significant infringement of the rights of another person. The classic examples of this are yelling “FIRE” in a crowded theater, or committing libel or slander. In the case of technical data concerning encryption software that is already in the “public domain” (as defined in the ITAR for technical data), the damage (or benefit), if any, is pretty much already done and further publication probably makes little difference. I believe that any definition of what is a munition that makes the nation’s bookstores and libraries appear to be exporters of munitions is not just ridiculous, it is unconstitutional.

When I tried to get clarification from the Department of State on what the rules that they applied when performing their censorship role (Commodity Jurisdiction Proceeding) were, all I got back was two letters, one that clarified a point made muddy by a typo in the ITAR and gave no help beyond the ITAR itself, and one form letter that said that the Department of State would not deal with hypothetical questions (even though most of my questions weren't purely hypothetical).

This serious Constitutional question casts doubt on the enforceability of any of the regulations in the ITAR against any encryption software. It could be difficult to prove that the publication of a particular piece of technical data or computer program caused specific, measurable damage resulting from intentional export without a license (even if you could figure out who exported it). Yet, there cannot be any restriction to U. S. Citizen's freedom of speech and freedom of the press unless it can be proved that damage resulted from that speech.

3. National Security Issues

"National Security" means a lot of things. It means maintaining the integrity and safety of our Constitution, our people, our land, and our environment. It means the ability to defend ourselves against anyone or any thing that would seek to harm us. Our freedom, constitutional democracy, and fairness to all citizens are our greatest protection against internal threats. This gives us the strength and will to have a strong diplomatic, economic, and military force to protect us against external threats.

3.1. Signals Intelligence

In the context of encryption software, the most obvious connection to National Security (if you ask the NSA) is the impact on intelligence operations. In the process of spying on enemies, it is a lot safer to listen to what they are doing remotely than to send a person in to spy. The two main ways of doing this are (1) to listen to and/or alter signals that they generate for their own purposes, and (2) to listen to signals emanating from devices that we have placed for the purposes of listening.

3.1.1. Enemy Signals

Enemy signals may include telemetry, radio transmissions on various frequencies for various purposes, telephone conversations, computer data links of various sorts, etc. These all may provide some kind of clue as to what evil deeds they may try to perpetrate on us next, or may indicate significant vulnerabilities for us to exploit in war time. The enemy knows that we know this, and will probably try to protect at least some of their signals using encryption, deception, jamming, or data hiding (steganography).

It is possible that an enemy might use some of our own encryption technology against us. The enemy may either directly use a commercial product to hide the meaning of communications from us, or use some published technology originated in the USA and other free countries to build their own systems. They may also add their own secret innovations to what they learn from us. Of course, there is also the consideration that an enemy would prefer to use cryptographic technology of their own design. This would give them the advantage of not letting us know which algorithm they are using. It would also deprive us of the huge head start we have on cryptanalysis of things like the ancient Data Encryption Standard (DES). This may not be enough to stop me from protecting a proprietary cookie recipe with the DES algorithm (or the triple DES variant if the cookies tasted good and weren’t fattening), but it would be a significant consideration for a nation planning to bomb Pearl Harbor. DES is probably a bad example, since everyone on planet Earth who really cares already has a copy of a program that does DES encryption, or can get one in a few minutes.

Using a commercial product like a spread sheet or data base program that does encryption only as an extra feature against us is something of a problem for an enemy, since such products are not normally well suited to the applications needed in military and diplomatic situations. Imagine giving a field commander a laptop computer with a U. S. commercial spread sheet program on it to decrypt orders from his commander. I may underestimate the silliness of our enemies, but I don’t think that this is likely. A much more tamper-resistant device with better key management would be much more appropriate for a military or diplomatic application. Use of our publicly available encryption design technical data in building more appropriate military communications security devices is a more likely threat in the case of a clever adversary. The only consolation in this case is that we also have access to this same data as an aid to cryptanalysis.

In the extreme case, strong cryptographic technology could become so readily available and easy to use that most of the interesting signals generated by enemies for their own purposes are encrypted in such a way that we cannot decrypt or subvert the communications without stealing their keys. In that case, all nations might have to behave like gentlemen (and not open the other’s mail or read their electronic communications). Then again, that is probably too idealistic to expect. It is more likely that mankind will only figure out other ways of spying on each other.

3.1.2. Bugs & National Technical Means

Even if the enemy takes great care to protect the secrecy and integrity of their own communications channels, we can still spy on them. Listening devices can be made so small and have such inconspicuous output that they can be almost impossible to detect or jam when planted properly. It takes very little power to send a signal to a nearby relay to a satellite, and many varieties of listening devices can be used. Even if an enemy becomes wise to one kind, another kind may be in use. Suffice it to say that all the encryption technology in the world could not cut off this source of intelligence, since all valuable intelligence exists in the clear at some point. If it didn’t, it would be of no value to the originator and intended recipient.

Public use of strong cryptographic technology may limit the points where listening devices must be planted to be of value, but can never totally cut off this sort of intelligence. Increases in knowledge cryptography and steganography may help this sort of spying more than hinder it.

3.2. Counter-Intelligence Activities

Increased public use of strong cryptography makes it easier for a spy to obtain a good cryptosystem. It also makes it easier to send encrypted messages without arousing suspicion. That is good for our spies, but bad for detecting spies in our own country. Then again, it would be a pretty inept spy (ours or theirs) who could not now obtain a good cryptosystem and send messages home without arousing suspicion, under conditions much worse than the USA right now. Of course, increased public use of strong cryptography also makes it harder for a spy to find valuable data to send back home. I think that the net effect will be that spies in the USA (and some other developed nations) will be harder to catch, but less effective.

3.3. Our Military and Diplomatic Communications

The greatest contribution of cryptography to our National Security is in protecting our own military and diplomatic communications from eavesdropping or alteration. Communications of this nature must be private, must be authentic (not an alteration or forgery), and must not have been altered in transit. Increased public use of strong cryptography can only help us to keep our most sensitive communications private. This is because there will be more encrypted traffic to attempt attacks on, making traffic analysis harder. It also may be that discoveries made in the private sector help in the design and evaluation of military and diplomatic cryptosystems.

3.4. Banking Transactions

We do so much banking electronically that failure to use strong cryptography to protect these transactions would be criminally negligent. It would be like not locking the vault and bank doors and not posting a guard. The importance of the integrity of our banking system to our economic well-being is obvious. The cryptographic protection must also be economical, just as the bank buildings, vaults, and other security systems must be, or the banks will not remain competitive. We must balance the cost of protection with the value of what is being protected. Strong cryptography usually doesn't cost much more to implement than weak cryptography, and may save a whole lot of money if it can prevent some fraud.

3.5. Domestic Personal and Corporate Communications

Although there are strict and fairly consistent guidelines for the protection of U. S. Government classified information, the private sector is much more vulnerable. Some companies are very security conscious, but some are not. Those which are not are easy targets for foreign and domestic spies, either working for governments or competing corporations (or both). Encouraging good security practices in the private sector, including use of strong cryptography, use of good crosscut shredders, etc., makes the USA more secure against this threat.

Protection of personal communications with encryption is good for privacy, just as locks on doors and curtains on windows are. It becomes very important in some cases, such as when a battered person is hiding from a stalker that is still at large, or when coordinating activities that might attract criminals like shipping diamonds. Encryption technology can help reduce crime, just like dead bolt locks. Just as I prefer to manage my own dead bolt keys, I'd rather not be forced to escrow a master key to my data with Big Brother. This isn't because I do anything evil with my dead bolts or cryptographic software, but because I love freedom. This preference is nearly universal among users of cryptography, and the countries and companies that cater to this desire will have a big economic advantage.

3.6. Authentication in the Private Sector

Encryption technology is the only way to provide a signature on a digital document. Nothing is totally fool proof, but digital signatures, when done properly, are much harder to forge or refute than pen and ink signatures on paper. Electronic documents can be transmitted faster and with higher fidelity than faxes, and the ability to sign them will be a great aid to quickly and conveniently doing business with remote customers and suppliers. As contract case law and technology evolve, this will become more and more important to our economy.

3.7. Upholding the Constitution

Citizens of the United States of America have a right to privacy guaranteed by the Constitution’s Bill of Rights. This quaintly stated right to be secure in our papers and effects is highly cherished. The advance of technology has eroded privacy. Corporations like Tandy openly track their customer’s names, addresses, buying habits, then shower them with junk mail. Credit bureaus keep massive amounts of (often incorrect) data on people all over the country — information that is supplied to lenders and in the form of prescreened mailing lists for solicitors. Government organizations keep records of real estate transactions, census data, and other such records that are used by solicitors to pester owners of houses in selected neighborhoods. Hospitals keep your patient records on computer systems that can be accessed by many people. Cellular and cordless telephones are trivial to monitor without physically tapping any wires, and legislated privacy in these areas is unenforceable.

Strong encryption can bring back part of the privacy that has been lost to technology. No law can keep spies and criminals from listening to phone calls made over radio links (including microwave and satellite links for normal phone calls), but encryption can make those calls unintelligible to criminals and other unauthorized listeners.

3.8. Law Enforcement

The proper use of encryption technology by law enforcement officers helps deny knowledge of monitoring operations to criminals and fugitives. It helps them to keep records private and protect under cover agents. It helps prevent tampering and deception from being used against them in their own communications. Unfortunately, this is a two-edged sword. Strong encryption technology can also be used by criminals to thwart the efforts of law enforcement officers to gather useful information from court authorized wire taps.

Strong cryptography also provides a “safe” way for a criminal to keep records of nefarious deeds that cannot be read by the police and used as convincing evidence leading to a conviction. Of course, fewer such records might be kept in the absence of strong cryptography, and some records kept in this manner might not be all that useful in obtaining a conviction. This is not very assuring to law abiding citizens and law enforcement officers, who want dangerous criminals to be caught well before they meet the Ultimate Judge in Heaven. Fortunately, most of the investigative tools available to law enforcement officials are not affected by strong cryptography. It is also likely that anyone stupid enough to engage in criminal activity is likely to screw up in some way that leaks information about their actions. Murder, terrorism, rape, and other violent crimes are not all that hard to commit (for those devoid of conscience or with the twisted conscience of a kamikaze), but these crimes are very difficult to get away with.

3.9. Technology Base Migration and Loss

When a technology is discouraged by over-regulation, taxation, or other means, that technology becomes less profitable in the country where it is discouraged. Less profitable technologies are not invested in as heavily. Therefore, the technology in that country will tend to fall behind. Right now, it appears more profitable to develop an encryption product for sale in many other countries than in the USA because export of this technology from the USA is discouraged but import is not. An entrepreneur in New Zealand has an unfair advantage against one in the USA. The New Zealander is not required to cripple key lengths or deal with unreasonable and unreadable regulations like our ITAR. This means that encryption technology in the USA will tend to atrophy while it prospers in other countries. This is bad for National Security.

4. Technology Issues

Any policy concerning encryption software that is to make sense must take into account the realities of the current state of the art in the applicable technologies. Failure to do so could at best lead to confusion, and at worst do much more harm than good.

4.1. Availability of Computers

It doesn’t take a lot of computing power to perform strong encryption (locking data up). It often takes a great deal of computing power to do serious cryptanalysis (unlocking data without the key). Strong encryption can be done with almost any microprocessor on today’s market. The original IBM PC (now greatly outclassed by the current desktop computers) has more than enough computing power to lock up significant amounts of data so tight that all the spy organizations in the world combined could not unlock it for thousands of years or more. This class of computer is available in essentially any developed or semi-developed country in the world.

4.2. Telephone Lines and Modems

There are still places in the world that don’t have easy access to telephone lines, but they are growing fewer all the time. The places that do have telephones, computers, and modems are those places where encryption technology is the most useful. Be they friend or foe, these places all have one thing in common. They are only a telephone call or two away from strong cryptographic software if they know where to call, and it isn’t that hard to find out. Since many telephone connections are by satellite, and since international telephone traffic is not routinely monitored and censored by most free nations, any technical data (including encryption software) can be transmitted across almost any national border unhindered and undetected.

4.3. The Internet

The Internet has grown to such a large, international collection of high speed data paths between computers, that it has become, among other things, one of the most effective examples of international freedom of expression in existence. Physical distances and political boundaries become irrelevant. I can peruse data posted for public access on university and corporate computer systems on five continents and many islands, no matter if I’m in the USA or in Russia. This is a powerful research tool. News groups provide discussion forums for subjects technical and nontechnical, decent and obscene, conservative and liberal, learned and ignorant, from Animal husbandry to Zymurgy, and more. The Internet provides easy access to lots of strong cryptographic technology and software that can be reached from any nation with a connection to the Internet. A great deal of this data originated from outside the USA.

The most complete and up to date collections of encryption software on the Internet are published for anonymous ftp from sites outside the USA. (Anonymous ftp sites are computer systems that allow anyone to log in with the name “anonymous” using the file transfer protocol program called “ftp” to transfer files to their own system). There are several ftp sites in the USA that carry some encryption software, and they have varying degrees of barriers to export. Some sites make no attempt at all to limit access to encryption software. Some sites are very effective at not allowing export, but are totally ineffective at distributing software domestically because of the hassles they impose on users (who can just as easily get the same stuff from Italy).

The strongest barrier to export that I've seen used at a U. S. domestic ftp site for encryption software that doesn't totally defeat most of the advantages of this form of software distribution is the one used at rsa.com for the distribution of their RSAREF package and RIPEM. The idea is to force you to read a text file containing an anti-export warning before you can find the data you are after. The text file that contains the warning also contains the name of a hidden directory that changes periodically. The encryption software is in the hidden directory. Naturally, this doesn't prevent an unwelcome intruder from stealing the data anyway, but the moral barrier presented probably reduces the number of "exports" from that site initiated by people in other countries. I support RSA Data Security, Incorporated's right to publish this data, even though I have observed copies of this data on several foreign computer systems.

I tried hard to think of a better solution (and even called the Department of State and the NSA for ideas), but there is basically no way to widely and freely publish any data in the USA without making it possible for a foreigner to steal that data out of the country. Even if the data is confined to physical packages and sold or placed in libraries only in the USA, there is nothing to prevent someone (either a U. S. or foreign citizen) from buying or borrowing a copy, then transmitting a copy of that copy out of the country. Even if positive proof of citizenship is required before release of the data, all it takes is one citizen to release a copy of the data outside the USA. You might argue that there would be a strong moral barrier against this, but remember that all it takes is one. What does it matter to someone if they send a copy of encryption software to a friend or relative in another country so that they can send private electronic mail back and forth? All it takes is one copy out of the country, and that copy can be copied any number of times. If rabbits multiplied so easily, we would all quickly drown in them.

The bottom line is that the best solution to balancing freedom of the press and the ITAR for encryption software ftp sites is just an annoyance for the intended users and a way to make it impossible to prove that the operators of the site intended to break any valid law. This may or may not have any bearing on the proliferation of encryption technology outside of the USA. I am not a lawyer, but I know RSA Data Security, Incorporated, has lots of them, and I don't believe they would do anything stupid.

4.4. Information Services and Bulletin Boards

CompuServe, America Online, Genie, Bix, Delphi, and other similar services offer massive amounts of data, including encryption software and technical data, to callers. They often act as common carriers between correspondents who carry this data themselves, and really don't know the contents of what they are carrying. Other times, they are well aware of what they have. For example, CompuServe publishes a magazine promoting some of the shareware that they carry, and featured some encryption software in an article in their November 1993 issue. These information services also serve customers outside of the USA. Indeed, it would be very difficult not to do so, even if they didn't want to bring some foreign money into their hands.

Computer bulletin board systems vary in size from hobby systems running on a single PC in a home to large commercial systems. Some are run as a hobby, some as a means of providing technical support to customers, and some as profit-making information services. A very large number of these systems have encryption software on them with no export controls expressed, implied, or implemented. Indeed, many of the operators of these systems would laugh in your face if you claimed they were trafficking in arms. These systems are normally accessible from anywhere with a telephone, computer, and modem.

4.5. Books and Magazines

Encryption software and technical data about it can be found in a large number of books and magazines in libraries, book stores, and by subscription in and out of the USA. Some of these have companion disks that can be ordered separately or that are bound in the back of the book. Some have associated postings on an information service. Some have printed computer program source code listings in them. In those rare cases where the book and disk sets are not distributed by the publisher outside the USA, it is almost certain that the books and disks will appear outside the USA, because most book stores don't restrict their sales to U. S. Citizens. Indeed, to do so sounds rather fascist and unamerican: "Let me see your citizenship papers before you buy a book!" This country is both more pleasant and a lot more secure without such nonsense.

4.6. Availability of Encryption Software

There is already a large number of free or very inexpensive software packages available internationally from various information services, computer bulletin boards, Internet ftp sites, and commercial packages available off the shelf. These include:

☞ Many DES implementations originating from many countries.

☞ Several packages that implement the Swiss IDEA cipher.

☞ Several packages that directly implement triple-DES.

- ☞ Assorted implementations of published algorithms, some of which probably exceed DES in strength.

- ☞ Assorted programs (such as utility packages, spread sheets, database programs, and word processors) that include some form of encryption that is incidental to their main function. The security of the encryption varies from so poor that it should be called false advertising (like that used in Microsoft Word), to probably good against all but professional cryptanalysts (like PKZIP), to fairly decent implementations of DES or better.

- ☞ Numerous proprietary algorithms, many of which probably claim greater security than they merit, but some of which may be very good.

- ☞ A few encryption packages that effectively use a combination of the RSA public key encryption algorithm and a block cipher (DES, triple DES, or IDEA) to encrypt electronic mail.

- ☞ Several cryptographer's tool kits that implement large integer arithmetic over finite fields, fast DES, IDEA, and RSA implementations, and other data that facilitates including these functions in other programs.

There are also a few cryptanalytical programs floating around internationally to assist in cracking insecure cryptosystems like the password protected files of Microsoft Word and WordPerfect. In most cases, this software encryption and cryptanalytical software cannot ever be eradicated (even if you think it should be), because there are so many copies held by people who think that this software is a Good Thing. Any one copy can be copied again as much as desired. Hiding software is much easier than hiding elephants.

The bottom line is that the cat is out of the bag, so to speak, and no amount of regulation can ever put the cat and all its millions of kittens back in again.

4.7. DES is Dying

DES was doomed to a limited lifetime from the beginning by limiting its key length to 56 bits. This was probably done intentionally, since there was much opposition to this decision at the time. It is also possible that this key length may have been an indication from the NSA that because of differential cryptanalysis, the strength of the algorithm didn't justify a larger key. Now a paper has been published that shows how DES can be cracked for an amount of money that is within the budgets of many nations and corporations (*Efficient DES Key Search*, by Michael J. Wiener, 20 August 1993). Schematic diagrams of showing how to build a device to accomplish this task are included in the paper, which has been distributed internationally electronically. I would be very surprised if one or more of the world’s major intelligence gathering organizations had not already built DES cracking machines of greater sophistication than Michael Wiener’s. The only reason that I say that DES is not totally dead is that it is still useful in some cases, for the same reason that physical locks that can be picked with a pocket knife or credit card in a matter of seconds are still sold and used. DES encryption does help keep unauthorized, honest, ladies and gentlemen out of your proprietary and personal data. When used in its triple DES variant, it might even keep dishonest people with big budgets and lots of motivation out of your private data.

4.8. Unbreakable Encryption

One very well known algorithm (called the One Time Pad), when properly used (i. e. with truly random keys used only once), can never be broken by anyone, no matter what their computing power. The One Time Pad has been known to the general public for many years, but it has not caused the end of the free world. I’ve never heard of a case of it being used for any criminal activity except for spying (and there, I suppose, the use by “us” and “them” somehow balances out). The One Time Pad is still used to protect our most sensitive diplomatic communications. An implementation of the One Time Pad in software is trivial, as the following complete, non-hypothetical, Pascal program demonstrates:

```
program one_pad;
  uses dos;
  var infile, keyfile, outfile: file of byte;
    plain, key, cipher: byte;
begin
  if paramcount < 3 then
    begin
      writeln('Usage: one_pad infile keyfile outfile')
    end
  else
    begin
      assign(infile, paramstr(1));
      reset(infile);
      assign(keyfile, paramstr(2));
      reset(keyfile);
      assign(outfile, paramstr(3));
      rewrite(outfile);
      while (not eof(infile)) and (not eof(keyfile)) do
        begin
          read(infile, plain);
          read(keyfile, key);
    {The following single line does the encryption and decryption!}
          cipher := plain xor key;
          write(outfile, cipher);
        end;
      close(outfile);
      close(infile);
      close(keyfile);
    end
end.
```

The whole One Time Pad program is short enough to be written from memory (for an experienced programmer, anyway). (For instructions on using the above program, see your local library or check out the sci.crypt Frequently Asked Questions document on the Internet.) It could be argued that the trivial program above isn't a complete encryption system, since it doesn't do any key management.

Ladies and gentlemen, does this document contain a weapon of war or other munition, or is it just free exercise of the author's freedom of the press? Would the ITAR prohibit the export of this document or not? I claim that the U. S. Constitution specifically allows me to publish this document, no matter what the ITAR says.

5. Economic Issues

While it seems clear that it is impossible to exercise our right to freely publish encryption technical data and software in the USA and at the same time prevent its export, it is very easy to economically damage the USA with encryption export controls.

5.1. International Trade

It seems that the only encryption software that can be legally exported for profit from the USA is either (1) crippled to provide weak security (i. e. only a 40 bit key with RC-2 or RC-4), (2) limited in function to certain purposes that do not cover all market needs, or (3) limited in distribution to a limited market. Therefore, encryption software export is not a very lucrative field to enter. How can you compete with foreign competitors who need not cripple their products?

5.2. Cryptographic Competition

There are sources of cryptographic software outside the USA where the encryption software is not crippled, and is available at a competitive price. Given a choice, the full-featured, secure software is more likely to win. This means that other countries will grow in this area and the USA will suffer economically.

5.3. Domestic Chilling Effect

Export controls on encryption software discourage distribution of strong encryption software in the USA and encourage the weakening of domestic software to the same inadequate standards forced upon exported software. It seems better to buy (real or perceived) strong security from an external source than from a domestic, persecuted supplier. Even though it would be unconstitutional for the ITAR to disallow domestic distribution of encryption software, few people want to be harassed by the federal government or become a test case where the unconstitutionality of the ITAR is conclusively proven in court.

6. Regulatory Issues

The International Traffic in Arms Regulations are designed to make the world a safer place by limiting the export of weapons and military equipment. It also regulates classified or otherwise non-public technical data about those weapons. Most of the items regulated have a whole lot more to do with the objective of limiting arms proliferation than encryption software and technical data. The subject of this document, however, is limited to a discussion of the regulation of encryption technical data and software.

6.1. Clarity of Regulations and their Intent

For a regulation to be effective and enforceable, it must be clear. No one should be compelled to guess what the state requires or proscribes. Indeed, how could you be expected to follow a law you don’t understand? There should be a clear way of telling what is and is not allowed without having to submit an item for censorship. The intent of the regulation should also be clear, so that a citizen could reasonably understand what the regulation is for.

6.2. The First Amendment

The ITAR cannot override the Constitution of the United States of America, in spite of its current claims that indicate that it does. To the degree that it does violate the Constitution, it is null and void. Any limitation on the freedom of speech and freedom of the press of U. S. Citizens must be clearly linked with a severe danger or denial of rights to another person that can be proven in court. Worse things than encryption software have been upheld in court as Constitutionally protected expression.

When balancing defense and intelligence considerations with the U. S. Constitution, it is important to remember that (1) the whole point of defense and intelligence operations is to protect and defend the Constitution and the people of the United States of America, (2) the Constitution is the Supreme law of the land, and (3) federal officials and military officers in the USA are sworn to uphold the Constitution.

There is a theory among those involved in private sector cryptography in the USA that there is an official or semi-official policy of discouraging strong cryptography within the borders of the USA, while giving the appearance of supporting it. There is evidence to support this theory in certain documents recently obtained under the Freedom of Information Act by John Gillmore and released to the public. This theory also explains a whole lot of otherwise difficult to explain circumstances. Because such a policy, if openly stated, would sound stupid at best and like treason against the Constitution at worst, it is not openly stated as such. Export control regulations and patent law appear to have been used as tools to carry out this policy of discouraging strong cryptography for the general public. In the event this scandal is even partially true, then the policy must be reexamined. This policy might not exist, but some alternate explanations for some of the evidence is even more disturbing.

6.3. Enforcement

A regulation that cannot possibly be enforced is of questionable value, at best. Ideally, it should be possible to detect all violations and demonstrate beyond the shadow of a doubt to a judge and jury that the violation was perpetrated by a specific person or persons.

6.4. Consistency with Technology

Regulations cannot ignore technology, math and science. Regulations cannot redefine pi to be exactly 3, repeal the law of gravity, or stop radio waves at national boundaries. In the same way, regulations (like the ITAR) that treat public information like tanks, guns, and nuclear weapons make no sense.

7. Recommendations

So far, I have pointed out problems and considerations that cannot be satisfied concurrently. On the other hand, it is possible to do much better than current regulations do.

7.1. Reevaluate National Security Impact

A study of the total impact of public use of strong encryption software should be made that includes all of the considerations mentioned above, as well as classified data concerning just how much impact (if any) such software (which is widely available now and projected to increase in both quality and quantity) has on current U. S. and foreign intelligence operations.

7.2. Deregulate Publicly Available Information

Export controls on publicly available information, including encryption software and technical data, are not only ineffective, unenforceable, unclear, and damaging to U. S. business interests, they are likely to be ruled unconstitutional in any serious challenge. Deregulating this information would help the U. S. economy, increase the use of strong encryption software in the places where it does the most good, and have minimal negative effects. Since so much strong encryption technical data and software is available now, it is unclear if any additional negative effects would even be enough to measure. The desired effects of better security and technology in the USA and a healthier economy would, however, be substantial.

7.3. Deregulate Research and Publication

Research and publication of scholarly work in the international, public forums benefit the USA. The fact that this also benefits other nations does not diminish the value to the USA. This does not prevent the NSA from conducting classified research within its security boundaries that is not available to the international community. It does prevent the NSA or any other government agency from interfering with or discouraging any work in the field of cryptography outside its own facilities. The NSA should maintain technological superiority by its own merit, not by crippling all domestic competition.

7.4. Replace DES with Better Public Standard

DES is old and its key length is too short. The public wants a more secure encryption standard that is fully public and can be used in software implementations. The Swiss IDEA algorithm is one likely alternative, but it would be better if an algorithm that is royalty-free (like DES) could be made an official standard. Clipper/Capstone key escrow is not the answer to this need, although it might be useful within the Federal Government.

Several possible replacements for DES have been suggested. One that is much stronger than DES (and slightly stronger than IDEA) and can be used royalty-free is the MPJ2 Encryption Algorithm, which has been donated to the Public Domain by the inventor. Technical details on this algorithm have been published, and are available to U. S. Citizens in the USA.

7.5. Control NSA's Cryptographic Technology

While it is unreasonable to think that the general public's cryptographic technology could possibly be confined to any one country, it is not so difficult to control the technology in a single organization such as the NSA. The NSA should be, with very few exceptions, a trap door for information on cryptography and cryptanalysis. They should strive to stay ahead of the general public in these fields, and should not confirm or deny what they can and cannot do to the general public without a conscious decision by competent authority to do so (for example, to endorse a DES replacement). In like manner, the NSA should not discourage or encourage any cryptographic technology outside of their walls but still inside the USA. Of course, even an endorsement by the NSA is suspect, since their charter includes reading other people's encrypted traffic. It would be better, in my opinion, to preserve the NSA as a national treasure of cryptographic expertise by dealing with public encryption standards totally within the Department of Commerce, National Institute of Standards and Technology (NIST).

It is probable that someone in the USA (or another country) will independently invent something that someone inside the NSA has invented, and that person will be honored with fame and fortune publicly for what has already been done privately within the NSA. This should never be construed as an excuse to censure the public invention. Indeed, to do so would leak information about the NSA's technology level and capabilities to the outside world.

7.6. Alternate Intelligence Methods

To mitigate the effect of the inevitable improvement in both the quality and availability of strong encryption software and hardware all over the world, it would be wise to invest in alternate intelligence methods, such as harder to detect and easier to place bugs. Subtle long range bug delivery mechanisms, relay devices, etc., could pay back great dividends in intelligence value for the money for use in those cases where strong encryption makes cryptanalysis impossible.

7.7. Alternate Law Enforcement Methods

There are many ways to catch a crook, no matter how cryptographically sophisticated. After all, it is much easier to plant listening devices around a suspected drug trafficker, serial murderer, or whatever, in our own country (with a proper search warrant) than it is to try to figure out how to bug the command center of an enemy dictator surrounded by a loyal army. An encrypted phone conversation may actually lull the bugged suspect into a sense of false security, talking openly about crimes on a secure line. An encrypted telephone does a criminal little good if the room or car the phone is in is bugged.

7.8. Clarify & Repair Export Regulations

My specific recommendations to clarify the export regulations with respect to encryption software, keep the encryption technology that we use for our own military and diplomatic communications safe, allow all reasonable commercial uses of encryption technology in the United States, to make the regulations much more enforceable, and to bring these regulations into compliance with the United States of America's Constitution follow.

§ 120.10 (1) should be altered (by removing the exception for software defined in a nonexistent section) to read:

> (1) Information which is required for the design development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation.

§ 121.1, Category XIII, subcategory (b), items (1), (2) and (3), should be modified to read (overly broad definition deleted and other changes underlined):

> (b) Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefor, including:
>
> (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 originated by the U. S. Government or persons working under contract to the U. S. Government, except for those specific items intentionally released by the U. S. Government to the general public or independently developed by a person or persons outside of the U. S. Government. In case of any doubt about the status of any of these items, see §120.4.
>
> (2) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software which have the capability of generating spreading or hopping codes for spread spectrum systems or equipment and which were originated by the U. S.

Government or persons working under contract to the U. S. Government, and not independently developed outside of the U. S. Government.

(3) Cryptanalytic systems, equipment, assemblies, modules, integrated circuits, components or software originated by the U. S. Government or persons working under contract to the U. S. Government, and not independently developed outside of the U. S. Government.

The above changes have the effect of maintaining strict controls on the cryptosystems that we use in our own military and diplomatic service, but has no ill effects on the U. S. Constitution or economy. It also has the effect of costing less taxpayer money to support censorship (Commodity Jurisdiction) proceedings.

§ 121.8 (f) should be modified to read (deleting the exception for encryption software):

(f) Software includes but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair. A person who intends to export software only should apply for a technical data license pursuant to part 125 of this subchapter.