Journal of Universal Computer Science, vol. 2, no. 3 (1996), 113-146
submitted: 10/1/96, accepted: 12/2/96, appeared: 28/3/96 *© Springer Pub. Co.*

Government, Cryptography, and the Right To Privacy

Jenny Shearer
(HyperMedia Unit, University of Auckland, New Zealand
jshearer@cs.auckland.ac.nz)

Peter Gutmann
(Computer Science Department, University of Auckland, New Zealand.
pgut01@cs.auckland.ac.nz)

Abstract:
The notion of a right to privacy of citizens in their communications is discussed in the context of an international movement by governments towards regulation of cryptography, and consideration of key forfeiture systems in national cryptography use. The authors argue that the right to privacy in communications networks is an issue of major importance, assuring freedom of the individual in national and global communications. Regulation and control of cryptography use on the Internet by national governments may lead to an imbalance in the citizen/government power relationship, with sequelae including unprecedented surveillance of citizens, disruption of international commerce due to lack of powerful cryptography (and lack of standardisation), human rights abuses by less democratic or non-democratic governments, and limiting of the political potential of an Internet global political system.
Category: K.4.2 Social Issues [Computers and Society]; K.5.2 Governmental Issues [Computers and Society]; E.3 Data Encryption

1 Introduction

Cryptography use within the Internet has the potential to reorder citizen/government power relationships, a potential which is already attracting the close attention of national governments. Cryptography policy in the United States is the subject of low-level controversy, following the failure of the "Clipper" initiative, where the Government attempted to introduce a key forfeiture system. The EC has considered banning the public use of "strong" cryptography. The power shift initially appears to be due to uptake by Internet users of easy-to-use, freely available, effectively unbreakable cryptography. The result: completely private domestic and international communications, with the promise of follow-on "untraceable" digital cash. In response, governments are formulating policy with an unspoken subtext, which is a strong perceived interest in controlling cryptography use. The issues are major: economic advantage, national security, and law and order. How the balance of governmental controls and citizens' rights is resolved could have important political and economic consequences. The emerging scenario appears to follow on from a traditional "national" perception of cryptography as a weapon to be used in times of war, for secure communications by spies and the military. This paper will argue that not only has cryptography moved from the shadowed domain of confidential defence dealings into the public arena, but also that a raft of new issues are involved, for

example the novel clash between the interests of sovereign nations, and "global" interests of the increasingly politicised Internet community.

In unravelling the complex issues involved in cryptography, it is helpful to look at three separate, though related, perspectives: those of the state, the market, and the citizens. In this way it is possible to weigh up the tradeoff of advantages and disadvantages to each group. So far, the gains and losses to national interests have been presented by law enforcement agencies as key matters in discussions of legislators in the US and in Europe. However issues across the board from human rights to small business security are potentially affected by the attitude taken by national legislators to cryptography.

Cryptography is central to questions about how free the citizens of the future are going to be under the conditions of the future Internet. Development in the United States appears to be heading towards a push by a few large companies to a one-way channel to consumers of information as a commodity: home shopping, movies, packaged information for areas such as education and health [Johnson 1995]. The Internet as marketplace requires cryptography only as a means of keeping commercial transactions safe: it is in the area of political discussion and other public forum functions that the importance of cryptography as a social issue becomes apparent. The Internet offers piecemeal information, and may lose out to large commercial information providers because of this. However, it already offers a politicised environment where newsgroups and lobby groups actively inform the Internet "community". This function may be seen as an important new "public good" which possesses potential for a global public forum. Its point of vulnerability in political terms is that it operates under a system where internal control is extended only to technological structures and necessary bureaucratic measures. Internet users are, in fact, highly vulnerable to the placing of national "security" measures which may impact heavily on individual privacy.

Privacy of communications is not considered to be a human "right" in most countries as, for example, it is argued in international forums literacy should be a human "right". The Japanese constitution is unusual in guaranteeing citizens privacy of communications (Article 21 of the Japanese Constitution states in part "No censorship shall be maintained, nor shall the secrecy of any means of communication be violated", making Japan one of the few countries with constitutional guarantees of privacy). The authors are arguing that privacy of communications should be assumed to be a "right" of citizens, unless governments can produce instances in which national interest may rationally be found to override the "right to privacy" of citizens. We would argue that citizens should appropriately take a keen interest in any arguments put forward by governments to make exceptions to the right to privacy. The technology of the Internet is outstripping the capability of ethics developed on a global basis, for example, to create a global viewpoint on the balance between privacy needs and national and economic interests. The outcome is the potential for infringement of personal privacy on an unprecedented scale, a phenomenon which should not be viewed with complacency in even the most "free" societies. Strenuous efforts put in by national security

services to increase surveillance over citizens have been documented in the US, a situation which has led to concern in a society which considers itself to be one of the freest in the world. After all, if people are going to communicate and conduct business every day on the Internet, much as they used to over the fence or at work down the road, they will wish to do this without eavesdropping by the neighbourhood busybody. In the years since Orwell's "1984" was published, the term "big brother", representing a government which wishes to maintain total surveillance and control over citizens, has become a modern cliche. This book created a sense of outrage when it was published, but in an era when surveillance techniques are beginning to approach those of Orwell's imagination, a desensitised population is failing to protect a traditional, and vital personal freedom.

The implications of loss of communications privacy are major concerns for human rights, for example in countries where oppressive political regimes find an interest in maintaining the fiction that all subjects agree with their views. The takeover of the Internet, juxtaposed with a political regime intent on using covert surveillance measures to monitor dissent and track the activities of people considered suspect, could smother political dissent, a goal which has been aspired to many times historically, but never before achieved. Most local area networks may be perceived as "spy networks" in which each node watches all the information flowing over a shared wire and picks out only those messages intended for it [McLeod 1993]. It takes only a minor modification (such as putting an ethernet card into promiscuous mode) to allow one machine on the network to watch all information for all machines on the network. When used in a firewall situation, a 486 PC can handle packet filtering at full T1 bandwidth [BorderWare 1995] meaning that a single PC discreetly inserted anywhere along the long link tying a geographically isolated country like New Zealand to the rest of the world can undetectably monitor all Internet traffic for the entire country. Given the low cost involved — a one-off investment of a few thousand dollars — and the scope of the possible return on this investment, it is clearly a temptation for governments to perform this kind of surveillance. The potential problem is not isolated to oppressive regimes, but is likely to appear in a different (illegal) form in traditional democracies, where citizens traditionally place a high value on privacy. The implications are wider than someone being annoyed that their financial status has been leaked to a wider audience than they would like, or that they appear on a consumers mailing list they don't want to be on. The implications for the less secure democracies are considerably more sinister.

1.1 Data Security

Data security without "strong" cryptography is problematic, and the United States, playing from a position of strength in the area of cryptography development, is providing an example of a country which is strongly favouring its perceived interests as a national government, but not entirely at the expense of refusing to listen to the concerns of its citizens. Thus in the United States cryptography is classed as munitions and hardware or software implementations are not allowed to be exported [Department of Commerce 1980] [Roberts 1988] [Department of State 1989] [NAP

1991] [Root 1991] [Department of State 1992] [Relyea 1994]. However, "strong" cryptography and Public Key Cryptography (PKC) is available for use within the US, and in a very restricted manner, for communications to US interests outside the country.

With the development of public awareness of and debate on government surveillance measures in the US, we see the emergence of a more mature understanding of the significance of cryptography. However, despite significant victories for the "electronic civil rights" lobby, the issue remains unresolved, with a central issue of a key forfeiture system (this term is used instead of the alternative 'key escrow' since it more accurately describes the act of involuntarily surrenduring privacy safeguards to an external agency) still being pushed by US Government agencies. The covert regulation of encryption by governments has generally been more comprehensive and more successful than any overt regulation. This covert regulation takes the form of patent secrecy orders on cryptographic patents, the cutting off of funding for research into promising areas of encryption technology, the discouragment of standardisation attempts for encryption systems, and documented harassment of providers of encryption technology aimed at ensuring they stay in line with government thinking. Americans, with a traditionally strong interest in protecting individual freedom, are confidently attempting to create a balance between the rights of the citizens to privacy and the control of terrorists, drug dealers, and so on. How the US decides these issues may be a useful lesson to other nations.

It is by no means certain the American people will tolerate the imposition of a key forfeiture system, and in the absence of this policy in the US it may be viewed as a very risky venture in terms of democratic politics for any other nation. That it is being seriously considered in legislatures as far apart as Australia and Europe indicates the extent of misunderstanding of the cryptography phenomenon (an example of this was illustrated by a recent call in the German parliament for a ban on encryption devices targeted at the level of encryption technology which existed before the second world war [Schroeder 1995]). The two methods which have been suggested to date, key forfeiture and weak encryption, are deeply flawed. Both schemes appear to negate most of the protection gained by encryption. The first, key forfeiture, requires trusted agencies who will hold the keys. To date no acceptable agents have been found. The main reason for this is the somewhat dismal record of existing government agencies which hold records on citizens. For example, the General Accounting Office (GAO) has stated that the FBI's computerized National Criminal Information Center (NCIC), established in 1967, is "routinely" used for unauthorized purposes by federal, state and local agencies [McPartlin 1993] [Madsen 1993a].

In San Jose, in the US, it is claimed police officers have sold information on individuals obtained from the mammoth Criminal Justice Information System system for $25 per report [Mercury News 1993]. The situation is little better outside the US. In the UK, many banks allow tellers to access any customer account; the information is then sold to anyone willing to pay for it [Luck and Burns 1994].

In Australia, the New South Wales Independent Commission Against Corruption (ICAC), conducting an investigation into allegations of widespread unauthorised access to personal data, found that information from a variety of State and Commonwealth government sources and the private sector had been freely and regularly sold and exchanged for many years. The organisations involved comprised a virtual who's who of Australian banks and insurance companies, as well as Australian Customs, Australia Post, the Department of Immigration, the Department of Motor Transport, the Department of Social Security, the Police, Telecom Australia, and various local councils and other government bodies [Clarke 1992]. The commission concluded that ".. a massive illicit trade in government information ... has been conducted with apparent disregard for privacy considerations, and a disturbing indifference to concepts of integrity and propriety ... Laws and regulations designed to protect confidentiality have been ignored ... [Even where criminal sanctions existed] information ... has been freely traded". In light of such reports, public confidence in key foreiture systems is likely to be, quite properly, low — as one writer was moved to comment, "trusting the government with your privacy is like having a peeping tom install your window blinds" [Barlow 1994].

An alternative key forfeiture proposal involving non-government agencies has run into similar problems. For example Bankers Trust, one of the organizations in favour of key forfeiture and who would like to become commercial key escrow agents, have recently been accused of massive fraud and corruption — with 6,500 tapes and 300,000 pages of written material as evidence [Business Week 1995]. Even taking the ultimate step of using the military as escrow agents is problematic because of the long history of cryptographic equipment and keys — exactly the material which is meant to be kept secret in key escrow — being leaked to outsiders, often for trifling rewards [Allen and Polmar 1988] [Polmar and Allen 1989] [Blum 1987] [Barron 1987]

The second of the two methods, weak encryption, is equally problematic. The main objection to this means of encryption regulation is that any encryption capable of being broken by the government is equally capable of being broken by any other government, or by large corporations, or organized crime, or a drug cartel, or even a student with access to some spare computing time. The largest publicly admitted application of computing power to cryptanalysis was the factorization of RSA-129, a part of the 1977 RSA Challenge [Atkins et al 1994]. This effort consumed 5000 MIPS-years of computing power over a period of 8 months (it is estimated that the same result could be obtained in about a quarter of the time using a somewhat better algorithm [Lenstra and Lenstra 1993]). With a little added financial incentive, specialised hardware can be obtained to speed up the task (for example an add-on card for AT-class PC capable of giving it a multiprecision math performance somewhat better than a four-processor Cray XMP cost about $4,500 in mid 1992 [Dubner and Dubner 1992]). The RSA-129 effort, carried out on a purely volunteer basis mostly by students, is more than many governments would be willing, or even able, to commit towards breaking an encryption scheme. This problem is further complicated by the steady advance of available computing power. Encryption which is rated as "weak" today will be classed as "laughable" in a few years time when

more powerful computers become available (it has been postulated that the easiest way to break an encryption scheme requiring the investment of 30 years of computing time is to do nothing for 29 years, then break it in 1 year using the computers available at that time). Since secrets worth encrypting will often need to be kept confidential for years, even decades, it seems futile to try and protect them with a scheme which will be broken within the useful lifetime of the secret they are meant to keep.

Banks and similar organisations already send huge amounts of data in encrypted form over electronic networks. Providing the ability to decrypt such data is an open ticket to commit financial fraud, and both weak encryption and key forfeiture encryption open electronic commerce systems to fraud. The same applies to electronic payment systems, where the use of this form of encryption is roughly the same as giving an attacker a blank cheque which can't be stopped and which has no withdrawal limit — once a secret key is compromised, there is no way to "un-compromise" it, leading to few limits on potential fraud. Similarly, industrial espionage is already big business and will only get bigger, and with bigger rewards come bigger temptations, so that attackers with the ability to decrypt sensitive communications and stored data are a very real threat and security liability for companies. The potential for damage is not limited only to financial and business information, but extends also to areas such as medical and personal data. For example, UK doctors guard their patients medical records with some care, and recently refused to put them online in unencrypted form as was called for in a national plan. Weak or key-forfeiture encryption would allow medical records to be accessed without the permission or knowledge of both doctors and patients, raising serious privacy concerns.

1.2 Political Implications

What are the reasons for the chaotic international situation regarding cryptography?

Democracy, shown to be a relatively fragile institution with a history of only a few centuries, may not have the legal and political structures in place to cope with the massive changes to information transfer which will result from the Internet becoming the new universal means of conducting human affairs, business, and personal, and political communications. The cryptography issue is a primary case in point. Citizens are required to cope with a new perception of cryptography, formerly the domain of defence egg-heads and highly classified usage in times of war or national danger. The risk is that public opinion, an important part of democratic structures, may not "operate" in the area of cryptography, because of public ignorance or a tradition of entrusting "military" matters to governments. Yet, if the governments move to compose legislation protecting "national security interests", or promoting further convenience or power in their own operation, they may trip over major emotional values of their citizenry: those pertaining to individual freedom. These values may not be articulated by a majority of the population, but will show themselves when the invisible "line" is crossed. A conflict already exists between

users of cryptography demanding complete freedom of use, and the pragmatic following of economic and security agendas by governments.

In terms of the argument relating to cryptography, governments should not perceive citizens as merely the geographic collection of people under their governmental control. While devolving state functions, limiting the power of labour unions, and so on may have modified a number of traditional pathways for influences on state policy, other loyalties and ties have developed. One of these is the feeling of "community" Internet users have towards the Internet. To limit effective use of the Internet by restricting access to cryptographic techniques, or by blocking the development of global standards, governments risk collectively offending users of the global Internet, on the grounds of loss of individual privacy and data security, and on grounds of inhibiting global commerce.

The issue, as yet something of a "sleeper" outside the Internet, is likely to develop as the Internet community gains some control over some of the more high-profile problems such as hacking and material considered harmful. Cryptography regulation may increasingly be seen by national governments as a means to control the new medium, as the Internet takes on its own identity in the area of mass communications, discussion forums and information systems, and digital commerce and digital cash move past the experimental phase. At this point, the effects of government regulation of cryptography use will become evident to the citizens, as a major control on their personal freedoms and privacy. Such regulation could also have the flow-on effect of limiting the potential of the Internet as the means for a global political movement. How the Internet community itself perceives the potential uses of cryptography is likely to affect how strenuously cryptography is defended by the community, as a means of achieving individual privacy, establishing a digital marketplace, and creating new political pathways via the Internet.

2. The State - National Cryptography Policies

2.1 The United States

The overt regulation of cryptography in the US is done through the classing of cryptography as munitions. Interestingly enough, the Internet itself was created as a munition, a "reliable means of transmission during events of unreliability", more commonly known as a nuclear war. Export of encryption technology from the US is occasionally allowed for large financial institutions which can prove it will only be used for data authentication purposes, or if the encryption is deliberately crippled to make it easy to break. Although the US government claims that "anyone can apply to export encryption technology", noone has ever been allowed to export anything other than very weak encryption systems (it is generally accepted that if any encryption technology is approved for export by the US government then it can't be any good. However, the converse is not true — unexportable crypto isn't necessarily strong).

An example of weakened, exportable encryption technology is Netscape Communications' World-wide Web browser, which generates a unique 128-bit session key for a transaction which is then used with a fast encryption algorithm known as RC4 to protect the rest of the transaction. To comply with US export restrictions, Netscape transmits 88 of the 128 key bits 'in the clear' along with the message, so that only 40 bits of the session key are actually kept secret. In July 1995, a French student used spare processing time on around 120 computers to break an encryption challenge posted to the Internet, in 8 days [Sandberg 1995] [Arthur 1995]. The attack was essentially "free", using only idle processing time on the machines. This type of attack can be mounted using spare processing time on machines available in universities, schools, companies, and businesses (for example one suggestion has been the creation of an encryption-breaking screen saver for machines running Microsoft Windows which recovers encryption keys when the machine is otherwise idle).

Another attack shortly afterwards took 32 hours, although it was estimated that a technical glitch caused it to take twice as long as it should have (a different attack, which takes advantage of an implementation flaw in the Netscape client software rather than the weakness of the encryption, takes about 1 minute on a cheap workstation). Another type of attack, which tests multiple sets of keys at once, is even faster [Collins 1995].

These successful attempts demonstrate the future security risk to businesses outside the US using weakened encryption. However the weak encryption does make the software acceptable to the governments of some countries such as France which normally ban encryption [DISSI 1995].

A number of attempts have been made to challenge the US export restrictions, both through attempts to change the existing laws via new legislation, and in legal challenges based on a claim that the ITAR contravenes the First Amendment to the Constitution, which guarantees freedom of speech [Kruh 1986b]. So far, all of these attempts have failed, on grounds of national security interests.

2.2 France

Like the US, France defines encryption hardware and software as munitions. The "decret du 18 avril 1939" defines eight categories of arms and munitions; the "decret 73-364 du 12 mars 1973" specifies that cryptography equipment belongs to the second category; the "decret 86-250 du 18 fev 1986" extends the definition of cryptography equipment to include software; and the "loi 90-1170 du 29 decembre 1990" states that export or use of encryption must be approved by the French government. A documented effect of the French ban on the use of encryption has been the increased ability of French intelligence agencies to perform industrial espionage on non-French companies operating in France. Foreign companies operating in France are required to register keys for any encryption systems they use "for reasons of national security". The head of the French DGSE (Direction Generale de la Securite Exterieure) secret service has publicly stated this

organisation helped French companies acquire over a billion dollars worth of business deals from foreign competitors in this way [Hellman 1993]. To thwart this, IBM at one stage routinely transmitted false information to French subsidiaries [Risks 1993]. The monitoring of communications by the French government has been going on for as long as electronic communictions have been around — as long ago as the 1860's the US Minister to France complained that "nothing goes over a French telegraph wire that is not transmitted to the Ministry of the Interior" [Bigelow 1909].

Admittedly, the US (and for that matter a great many other countries) are little better than the French in this respect. For example, in the late 1970's the CIA set up an "Office of Intelligence Liaison" within the US Department of Commerce to pass information obtained by US intelligence agencies operating listening stations in other countries on to US companies [CBC 1994]. There are two such stations operating in New Zealand, one at Tangimoana north of Foxton and one at Waihopai near Blenheim. Similar listening stations also operate in other countries, with their (mis)use for industrial espionage being admitted by US intelligence agencies [Markt & Technik 1994] or reported in the press [Reuters 1994]. Recently, there has been a scramble by US companies to take advantage of US intelligence capabilities for industrial and economic espionage purposes under a variety of euphemistic labels such as "strategic information acquisition" [Brod 1995]. The CIA, after restructuring in the 1980's, is now itself entering the field, providing their services not only to US government officials but also to organisations such as the Department of Agriculture and the Federal Aviation Administration (FAA) [CIA 1994].

2.3 Russia

In contrast to the long-standing French restrictions, the Russian ban on use of encryption was only recently introduced [Moscow Times 1995] [Rossiyskaya Gazeta 1995]. The Russian parliament refused to pass a law banning all encryption which was not approved by the Federal Agency for Governmental Communications and Information (FAPSI), a department of the former KGB, so it was enforced as a presidential decree instead. The decree instructs all commercial banks to conform to the decree in their dealings with the Central Bank of Russia, and instructs the Russian Federation Customs Committee to ban the import of any "encryption facilities" which don't have a FAPSI approved licence. However, the same technology which President Yeltsin used to stave off the attempted coup in 1992 is now being used to sidestep the ban on encryption, with non-KGB-approved encryption technology being freely available in Russia (for example a non-approved encryption library by one of the authors was made available by a Russian university as this paper was being prepared without any repercussions. As an old Russian proverb states, "The severity of Russian laws is compensated for by their non-mandatoriness"). The same appears to be true in France, where individuals freely use encryption software such as PGP.

2.4 Australia

In July 1995, the Australian Government tested the waters of encryption regulation in a curious paper which, although presented by the Assistant Director for Security Management of the Australian Attorney-General's Department in a session attended by representatives from the Australian Defence Signals Directorate (DSD) and the UK Government Communications Headquarters (GCHQ), was marked as being "the views of the author and not necessarily representing the views of the Australian Government" [Orlowski 1995]. In this paper the author, while repeatedly stressing that "users will not use cryptographic systems unless they have confidence in them" and that "confidence in encryption techniques and technology is pivotal to confidence in information infrastructures", then states that "I feel that the needs of the majority of users… can be met by lower level encryption which could withstand a general but not sophisticated attack against it". The paper did not explain how these two views might be reconciled.

2.5 Germany

The German government also appears to be moving towards restricting privacy technology. On 4th May 1995 the German cabinet passed the Fernmeldeanlagen Überwachungs-Verordnung, or telecommunications surveillance bill, which requires that almost all communications carriers provide a standardized interface to allow monitoring by government agencies. This covers telephones, cellphones, ISDN, and computer networks. Additional information such as call setup information and data to allow tracking of cellphone users within cells has to be made available. Finally, the creation of a universal database listing the users of these services is required [taz 1995] [Fox 1995]. According to a recent revision of the Telekommunikationsgesetz (TKG-E, or "telecommunications law") this surveillance must be able to be carried out in an undetectable manner, with only a bare minimum amount of oversight over the surveillance process being allowed [FIfF 1995]. Given that many intelligence agencies already have the capability to scan voice communications for individual voices and keywords (for example [CSE 1993]) using technology which is easily available (see for example [James 1995], which covers speech recognition and automatic topic classification with scanning for items matching an arbitrary expression of the information requirement) and that a recent change to the German G10 law specifically allows for this form of scanning, there is potential for large-scale automated surveillance of phone communications (an investigation arising from a law professors complaint that the law was unconstitutional revealed that currently all telex and fax transmissions are monitored, and that voice communications are scanned for keywords). Although employees of the German BSI security agency have privately expressed the opinion that an encryption ban would cause far more damage than good because of easier industrial espionage and that crypto software is essentially uncontrollable and will be used by criminals even if it is banned, it appears that sections of the German government are still working on encryption bans [Spiegel 1996].

2.6 United Kingdom

The use of encryption has been considered by various political parties in the UK, with most of them being in favour of it. The British labour party, after initially coming down against encryption on the advice of various governmental security advisers, changed their policy after feedback from Internet users so that their current position is that "attempts to control the use of encryption technology are wrong in principle, unworkable in practice, and damaging to the long-term economic value of the information networks. Furthermore, the rate of change of technology and the ease with which ideas or computer software can be disseminated over the Internet and other networks make technical solutions unworkable. Adequate controls can be put in place based around current laws covering search and seizure and the disclosure of information. It is not necessary to criminalise a large section of the network-using public to control the activities of a very small minority of law-breakers" [Internet 1995]. The leader of the UK Liberal Democrats similarly expressed the view that "encryption … is a good thing. It provides a form of security for business and for personal exchanges not unlike putting your message, cheque or whatever into an envelope. Individuals, be they acting on behalf of companies or for themselves should have the right to encrypt their messages as they see fit in such a way that only the intended recipient can decrypt it. Secure business transactions demand that electronic data (particularly financial data) should not be tampered with. There are some fringe activities, which need to be looked at, such as international crooks using the Internet to send their information about their intended actions. Telecomms operators, who merely provide the means for messages to be transmitted, need to be protected by law from prosecution for allowing (unwittingly) their infrastructure to be used by crooks, terrorists and vagabonds for planning illegal activities" [Lees 1995].

2.7 South Africa

Another example of partial regulation of encryption was South Africa, which in the mid 1980's passed a law that civilians could only use encryption if they gave the South African army not only full details of the algorithms and protocols, but also copies of all keys in use. The banks sent a message to Pretoria to say that they welcomed the idea of handing over the keys to their ATM's to the army, and that whenever any of them were out of balance at the end of the day they would send the bill to the government (banks use encryption primarily for legal reasons — the key used to derive the PIN from an account number and miscellaneous other information is kept in secure hardware, so no bank employee can ever find out a customer's PIN. Since the banks'security procedures are always completely foolproof and above reproach, the only way the balance could be out is if a dishonest member of the army had misused the keys held by the army to help themselves to some cash. Therefore it was only proper that the government foot the bill for this).

After a long silence, Pretoria gave an assurance that the banks could go on breaking the law and nothing would happen to them [Anderson 1994a].

2.8 Other Countries

A few governments have taken halfway steps towards regulating encryption. For example, the Norwegian government has introduced its own encryption standard called NSK, a secret stream cipher algorithm in a tamperproof chip which can only be used under tightly controlled conditions [Madsen 1994]. The Australian Defence Science and Technology Organisation (DSTO) and Defence Signals Directorate (DSD) developed the SENECA encryption device for use within approved government departments in Australia and New Zealand [PC Week 1993]. In both cases strict controls over distribution of the hardware would ensure government control over the encryption devices, making a key forfeiture mechanism redundant.

Other countries have also worked on tackling the "problem" of encryption technology. The Dutch government looked at banning encryption in 1994, but backed down rapidly over a storm of protest [Remijn 1994]. More seriously, a number of totalitarian states such as China (which recently required that all Internet users register with the police), Iran and Iraq are known to place heavy penalties on the unauthorised use of cryptography.

In general countries follow recent directives which replace the older COCOM rules restricting export of cryptographic hardware and software to a number of countries including the former Soviet bloc, to ones covering a much smaller list of countries such as Libya and Iraq (the members of this list change with time). An example is the Austrian law on foreign trade [AHG 1995] which follows the equivalent EU directive [EU 1995] almost verbatim.

3.The Standards Dilemma

3.1 The United States and National Interest

The US is retaining US developed encryption systems in its own hands, for "national interest" reasons. In economic terms, the US Government is evidently mindful of the penalties which may follow export and international use of encryption and encrypted commercial transactions on the Internet. The issue is overshadowed by the policy position of the United States, an unrivalled superpower with an economic system burdened by state overspending and high national debt. The vulnerability of the US economy in the event of loss of tax revenue, for example, has caused the issue of cryptography to become charged with multiple implications.

The United States has expressed commitment to the future of the information superhighway, of which the Internet is a major growth area. However,in the area of cryptography policy it is not surprising that the US Government is tending to regard the major problems which it is faced with as problems that will be solved by the US according to its national needs. In international relations terms, this means the US is appearing to place its national security interests and economic interests before considerations such as the best future development of the Internet or the economic

well-being of other nations. The time gained by retaining export controls on cryptography export may be essential time for the US to deal with the regulatory implications of digital commerce and to develop an effective working digital cash model, which may then be imposed on the Internet as a de facto standard. Policymakers are already showing signs of developing control mechanisms using software patents, and export bans on certain types of encryption. This "you want it, but you can't have it" scenario is not likely to advance the development of the Internet — partly because of time frames, and partly because the US is creating an encryption environment, intentionally or not, which dictates to users of the Internet how encryption will be used. Internet users of cryptography are advocating the dropping of controls over publicly developed cryptography, as Internet development is clearly penalised by the lack of distinction made between the various issues by US government agencies, and the corresponding lack of clear-cut issues presented for public debate.

3.2 Interoperability Problems

One of the main impediments to the widespread use of encryption technology today is the lack of any well-recognised international standards guaranteeing interoperability between different implementations. The sole internationally-standardised encryption algorithm, DEA-1 [ISO 1987] [ISO 1988a] [ISO 1988b] [ISO 1991a] [ISO 1991b] more commonly known as DES, was established over the strenuous objections of various security agencies (actually the DEA-1 algorithm itself is an almost-standard — after the DEA-1 vote, the ISO suddenly decided not to play a role in the standardisation of encryption algorithms). For example, on the day Standards Australia's vote on the DEA-1 ballot was to be decided on by the committee covering it, an individual who wouldn't identify himself but who claimed to represent the Australian Department of Defense appeared and circulated a document urging a "no" vote based on the claim that if it was standardised the Japanese would manufacture cheap equipment to the standard which would then be used by terrorists, drug dealers, and child pornographers (this never happened — here are only one or two DEA-1 encryption chips available to the public which are manufactured in Japan, and even these are rather difficult to obtain). The committee had trouble taking this document seriously, and the vote was 13 in favour, 1 against. However, when the Australian "yes" vote made it to Geneva, it had changed into a "no" vote. The NSA itself has called DES "the worst mistake the Agency has ever made", mainly because it gave a major impetus to two decades of research into encryption systems where before the "mistake" there was virtually nothing [Deavours 1987].

A similar battle occurred over the attempt to standardise triple-DES encryption in the US. DES had long been recognised as being past its prime [OTA 1987] [Smid and Branstead 1988] [Federal Register 1992], and a new triple-DES standard was seen as an attempt to prolong the life of the cipher into the next century [X9 1994]. Triple-DES is popular because it can be easily incorporated into existing systems using DES, is based on standards and procedures familiar to most users, and can be made backwards-compatible with single DES with an appropriate choice of keys.

The NSA circulated a document among the members of the ANSI X9 standards committee [Rainville 1994] urging a negative vote on the proposal based mostly on the fact that triple-DES is "counter to national security and economic concerns", a curious claim since the reasons for X9 working on the triple-DES standard were to provide better protection for financial information than that afforded by single DES. A few months later,work on the triple-DES standard was approved [CDT 1995a], providing a major setback for the NSA who were now faced with the threat of a standardised encryption algorithm providing more strength than the Skipjack algorithm used in Clipper, but without Clipper's key forfeiture mechanism. The availability of triple-DES implementations received a further boost shortly afterwards with the announcement by AT&T and VLSI Technologies that they were developing new data security products based on triple-DES. Triple-DES hardware had already been openly available outside the US for several years [Cryptech 1989] [CEI 1992]. However while trying to restrict the civilian use of encryption on the Internet, the US government has recognised the need for encryption by fielding its own encryption system for the transmission of classified documents, voice data, and video teleconferencing — by the US military only [Aviation Week 1995].

Government interference in encryption work is not confined to the US. The Sesame project, a clone of MIT's Kerberos designed to provide authentication but not privacy, had its DES implementation replaced with a 64-bit XOR (and even that, it turned out, wasn't implemented properly) at the insistence of the EU's Senior Officials' Group (Information Security) (SOGIS), which consists primarily of signals intelligence managers. Researchers on another project, RIPE [den Boer et al 1992] were paid to devise a hash function but forbidden to work on any form of encryption [Anderson 1995] When it comes to public-key encryption, government intervention in standardisation attempts have also been quite successful [Price 1989]. The result has been an almost complete absence of international standards covering the form and use of public-key encryption systems, and of encryption algorithms which can be efficiently implemented in software. The effect of this is that cryptographic privacy protection, where it exists, is of an extremely ad-hoc nature.

3.3 Privacy of Voice Communications

Frequently the issue of privacy protection through encryption is ignored entirely because nothing is easily available to perform the task. One situation in which this is glaringly apparent is in the cellular telephone industry. Analog cellular phones have no privacy protection mechanism, making it very easy to intercept conversations. Although the most widely-publicised means of interception are radio scanners, these present a needle-in-a-haystack approach to monitoring and make it almost impossible to target a specific phone or conversation. The best cellular phone interception device is another cellular phone. Details on converting cellphones to allow interception of calls are often available from the phone manufacturers [Motorola 1993] or are circulated in the computer underground [Bloodmoney 1992]. The process of converting a cellphone into a cellular scanner can take as little as 30 seconds (for example OKI 900 phones can be converted with 10 keypresses; many Motorola phones can be converted in a matter of seconds using only a paper clip).

The cellular phone industries response to this problem was to lobby the US Congress into passing the Electronic Communications Privacy Act [ECPA 1988], which requires people to pretend not to listen to the parts of the spectrum which contain cellphone traffic. Amusingly, some older television receivers with UHF tuning can tune the frequencies used by cellular phones, making it possible to break the law by tuning a television to the wrong channel (cellular phones operate on the frequencies formerly occupied by UHF television channels 70-83, which can be tuned by TV sets made in the 1970's or earlier).

Had low cost encryption technology been widely available then the cellular phone industry might have provided real security to their customers rather than the "security" provided by the ECPA, as well as avoiding some of the US $1.5 million/day losses incurred due to cellphone fraud [Wilder and Violino 1995]. The encryption used by GSM cellphones is another example of national interests taking precedence over genuine security. When GSM was being developed during the 1980's there was intense debate among the NATO intelligence agencies over whether the encryption used should be weak or strong. Countries like West Germany, which shared a long border with an eastern neighbour known for its strong cryptanalytic skills, wanted strong encryption. Countries like the UK wanted weak encryption. The result was an algorithm called A5, which has been characterised by UK cryptographer Ross Anderson as "not much good" [Anderson 1994b]. A simple brute-force attack requires searching 2^{40} keycombinations (the same number as the Netscape attack), with much faster attacks being possible. Interestingly, A5's low upper limit on the number of possible keys would seem to meet the US government requirements for weak exportable encryption. Attacks faster than the basic brute-force one are also possible, and one such attack was to be presented by Dr Simon Shepherd at an IEE colloquium in London on 3rd June 1994. However the talk was cancelled at the last minute by GCHQ. A chip to break A5 is currently being designed for an MSc thesis [Anderson 1994c].

However, even A5 was regarded as being too strong for export outside Europe. The result was a watered-down version called A5X, which was even easier to break [Lloyd 1993]. Countries like Australia, which managed to obtain cellphones employing A5 encryption, had to carry out multimillion dollar retrofits to communcations equipment to allow government monitoring of cellphone conversations [Lagan and Davies 1993] (the high cost of converting existing cellular phone networks into cellular monitoring networks has led at least one GSM vendor to claim that the cost of breaking GSM security itself was US$56M, this being the cost of the cellular network conversion as carried out in the Netherlands). Another alternative when governments find it impossible to monitor cellular communications is simply to ban them altogether [Griffin 1995].

3.4 US Government Covert Action in Cryptography Research and Development

Attempts to discourage research into encryption have occurred almost continuously for nearly two decades. In July 1977, NSA employee Joseph Meyer wrote to people planning to attend an upcoming symposium on cryptography that participation

might be unlawful [Pierce 1984]. In the summer of the same year, an NSA employee warned the inventors of the RSA cryptosystem against presenting a paper on their work at a conference at Cornell University [Garfinkel 1995].

In 1978, the NSA tried to block a patent on the Phasorphone, a cheap, simple telephone scrambler, but the secrecy order was revoked after an outcry in the media [Gilbert 1981] [LA Times 1994]. In the same year they tried to silence a University of Wisconsin computer scientist who had invented an encryption device [Kruh 1986a]. The chancellor of the university denounced the NSA for obstructing academic freedom, and the agency backed off [Markoff 1992]. In 1979, NSA Director Bobby Ray Inman, in an address which came to be known as his "the sky is falling" speech, called for encryption to fall under the same "born classified" doctrine which covers nuclear weapons research under the Atomic Energy Act of 1954 [Levy 1993].

In 1981 the American Council on Education (ACE), under pressure from the NSA, formed the Public Cryptography Study Group, which somewhat reluctantly recommended a trial scheme for the voluntary submission of crypto papers to the NSA as an alternative to the NSA's proposals that either the NSA monitor published technical information and recommend criminal prosecution if it was seen to threaten national security, or that the submission of technical papers to the NSA for prepublication approval be made mandatory, with publication without NSA approval being a criminal act [ACE 1981]. This scheme was again stopped by a media outcry [CFP 1994]. In 1982 the NSA tried to re-classify large amounts of previously public and declassified information used by James Bamford in his book on the NSA [Bamford 1982]. In 1984 National Security Decision Directive (NSDD) 145 gave the NSA authority over all government encryption and computer security development. In the same year the American Association for the Advancement of Science commissioned a series of ten study papers to investigate the ways in which secrecy and openness influence the conduct of scientific research [AAAS 1984]. In 1985 NSA Director for Communications Security Walter Deeley called for government regulation of encryption, stating that "it is time to put the genie back in the bottle for the good of society" [Deeley 1985].

In 1986 there was an attempt to extend NSDD-145 to cover the private sector. In the same year the NSA proposed a system in which they would provide all encryption equipment and keys for use in the US. This equipment would use NSA-designed classified algorithms with the special property that only certain types of keys would provide strong encryption, making it necessary to obtain all encryption keys from the NSA [Kolata 1986]. Opposition to this scheme was not long in appearing [Deavours 1986]. In 1989 the NSA attempted to stop dissemination of Ralph Merkle's "Khufu" encryption algorithm [Merkle 1991], one of the first very fast, secure software encryption algorithms (one of the authors has in his posession a yellowed printout of the Khufu paper, containing a hand-written note explaining it's "publication without NSA approval"). In the 1980's the National Science Foundation had a clause in its rules for graduate student fellowships requiring fellows to inform the NSF of any discovery "likely to influence national security". In June 1994, NSA agents visited

Jim Bidozs, president of RSA Data Security Inc, to talk about Clipper and RSADSI's competing products. After about two hours of discussions, one of the agents threatened to kill Bidzos because of the work his company was doing [Bank 1994]. A senior agency official later apologized for the incident, stating that it was not agency policy to make death threats.

Just how little things have changed in the encryption debate is shown by a dissenting opinion from a member of the ACE Public Cryptography Study Group, which raises a number of basic points which are just as valid now as they were fifteen years ago when the report was originally published [Davida 1981].

In addition to discouraging work on encryption products, the NSA has also worked to block any software which might somehow work with other encryption products. For example, in May 1995 the NSA requested that the capability to interface with external encryption software be removed from the NCSA WWW server [NCSA 1995]. Although the server contains no encryption code, the mere possibility that it might be hooked in at a later date were enough to attract the attention of the NSA. Similar problems have also beset other attempts at providing internationally-available encryption products by adding encryption capabilities outside the US [Walker 1994].

4.The Citizen

The Electronic Frontier Foundation was formed to champion the civil rights of computer users and to roll back a perceived attempt by the various arms of the US government to control what happens within the Net. The electronic civil rights movement has expanded to take in other issues, of cryptography, and wiretapping. The movement is questioning the need for extended state surveillance of private computer and telephone communications. For example when the FBI filed notice in the Federal Register in October 1995 requesting an increase by 1998 to one thousand times the number of taps officially carried out by the FBI in 1993, requiring that phone companies and other service providers build enough surveillance capacity into their systems that 1.5 million phone lines, or 1% of all lines in the US could be simultaneously wiretapped, calls isolated, and their contents forwarded to the FBI [Federal Register 1995], they were met by a storm of criticism in the US media, which raised the spectre of Big Brother and questioned the need for such a radical change in the surveillance capabilities of the government [Matthews 1995] [Markoff 1995a].

David Chaum, a pioneer of untraceable digital cash transaction technology on the Internet, places a high value on the privacy achieved by secure cryptography:

"The choice between keeping information in the hands of individuals or of organisations is being made each time any government or business decides to automate another set of transactions. In one direction lies unprecedented scrutiny and control of peoples' lives, in the other, secure parity between individuals and

organisations. The shape of society in the next century may depend on which approach predominates" [Chaum 1992].

Many of the problems associated with hacking may be prevented by use of encryption of information, which effectively sets boundaries around private, as opposed to public domains. Cryptography is used because of the risks of loss of security caused by hackers and criminals. Obviously, cryptography may be used by criminals or terrorists to formulate plans for crime or to actually carry it out. However, it could be argued much of current US policy making is the product of a particular mindset in regard to economics and security, and that the stated fear of US officials about encrypted computer crime may have limited justification.

4.1 The Clipper Chip

By late 1995, the US Clipper Chip initiative was generally acknowledged to have failed. The reasons for this have been covered exhaustively elsewhere, with two very in-depth discussions being [Hoffman 1995] and [Froomkin 1995]. The major objection to Clipper was that the proposed key forfeiture system was seen to be the forerunner to universal surveillance. Because of concerns like this, 80% of 1000 people surveyed in a Time/CNN poll were opposed to Clipper [Elmer-Dewitt 1994]. Anyone who wanted real security would either use something other than Clipper, or use Clipper to wrap up a second layer of non-government-approved encryption — as one commentator put it, "any self-respecting vice overlord or terrorist or local drug-runner … would buy non-American hardware with unmonitored Japanese or German or Indian encryption chips and laugh all the way to the plutonium factory" [Safire 1994].

Another problem with Clipper was the discovery by an AT&T researcher that the key forfeiture mechanism built into Clipper devices could be bypassed without too much difficulty [Blaze 1994] [Markoff 1994a] [Quittner 1994]. Clipper messages can also be "forged" without a need to know the encryption key [Lomas 1994].

A final nail in the coffin was the release to the Electronic Privacy Information Centre in August 1995 of declassified FBI files which revealed plans to outlaw any encryption other than Clipper [FBI 1993] [FBI Undated a] [FBI Undated b]. Although heavily censored, these documents still contain enough information to show that at the same time as the US government was publicly promising to keep Clipper as a voluntary standard [Harris 1994], it was secretly planning to outlaw any encryption which the government couldn't decrypt in real-time... unless that encryption was used by the government to protect its own secrets. These documents added weight to claims by anti-Clipper groups that Clipper would only serve its purpose if all other encryption were outlawed.

On 6 September 1995, the US government unveiled a new proposed crypto policy at a Key Escrow Issues Meeting [NIST 1995]. This policy gave 10 criteria which government-approved encryption systems would be required to follow, in return for making the resulting system exportable. The response to this proposal by

representatives of several of the largest hardware manufacturers and software publishers and various public interest groups was almost uniformly negative [CDT 1995b]. Clipper itself failed to meet many of the requirements, including (at least) No.1, No.2, No.5, and No.6.

The main problem with the proposal, quickly dubbed "Clipper II", was that it required both weakened encryption through the use of short keys, and key forfeiture. Several conference attendees claimed there is no legitimate purpose served by limiting the key length on a system for which the government already holds the keys. The short-key requirement was seen as an attempt to preserve an extra-legal alternative to legitimate access via the escrow agents, one which sidesteps any need for a search warrant or other judicial approval. Several of the other criteria (such as No.2, which prohibits multiple encryption) seem to reinforce this, making it possible for interested US government agencies (and well-equipped outsiders) to decrypt communications even without the escrowed key. It was also postulated that, since the 64-bit key is too small even for today, the whole Clipper battle could be re-fought in a few years time once attacks such as the current problems with Netscape's 40-bit keys are extended to 56-bit or 64-bit keys.

Another problem was criterion No.6, the requirement of non-interoperability with non-escrowed products, seen as yet another attempt to coerce key forfeiture without actually admitting to it directly. As with Clipper, it appears this requirement was designed to ensure that incompatible government-approved encryption would eventually flood out any competing systems. Yet another problem was that, as with Clipper, it was seen as unlikely that foreign governments would embrace a system which was conducive to US spying [EPIC 1995], especially in the light of evidence that the US had already in the past sold software with trapdoors in it to foreign governments [Madsen 1993b]. Finally, liability for compromised key databases was seen as a problem by a number of companies, with a Shell Oil representative stating that "the US government cannot cover Shells liabilities" in the case of compromised keys protecting data such as geologic information and market strategies, which were worth staggering amounts of money.

At present it looks like Clipper II may go the way of the original Clipper [Markoff 1995b] (Almost every non-government speaker at the Key Escrow Issues meeting prefaced their remarks with some form of "Do not assume our presence here is an endorsement, because it is not…". One speaker suggested having a t-shirt made up with this on it to save everyone having to mention it at the start of their presentation). The government representatives said that they heard the comments, but would proceed anyway. In an interesting reversal of the usual pattern of events, a group of 37 companies said they would formulate their own crypto policy and present it to the US government within six months [Corcoran 1995].

4.2 Cryptography Regulation

In the face of opposition to any form of government regulation of encryption and related invasion of privacy, it is interesting to speculate on the direction future attempts at encryption regulation will take.

The most difficult problem is proving that regulation is necessary. To date, governmental attempts at demonstrating a "problem" have been fairly unsuccessful, consisting of trotting out the so-called "Four Horsemen of the Infocalypse" (porn, pedophiles, terrorists, and drug dealers) as justification for encryption bans and increased surveillance powers over communications. These claims have been frequently challenged. For example, in a recent debate over Clipper, FBI Special Operations agent Jim Kallstrom attempted to justify Clipper by claiming it would help protect children from being kidnapped to make snuff movies [ABCNY 1995], seemingly unaware that another branch of the FBI had stated eighteen months earlier that snuff movies don't exist [Knapp 1993]. Similarly, when a major US paper published an editorial which called for a removal of restrictions on encryption, they could find noone in the FBI or Commerce Department willing to defend the government's position on encryption for the traditional Opposing View counterpoint piece [USA Today 1995]. Actual evidence to support encryption restrictions appears to be hard to find: Deputy Asistant Attorney General Robert Litt testified that the Department of Justice has no information or statistics linking any terrorist or criminal act to information derived from the Internet [Meeks 1995]; the FBI Deputy Director for Anti-Terrorism stated that he was unaware of any use of encryption by terrorists which would justify restrictions [Murray 1993]; and in a informal survey of front-line law enforcement officers carried out in May 1995 the question of whether there had ever been any problems with encryption hampering law enforcement was met with laughter from the agents questioned [Ellison 1995].

Even the claims of the need for greatly enhanced wiretap capabilities are somewhat questionable. For example in 1992 of the 39 states which have wiretap statutes, 17 reported zero taps that year; of the federal jurisdictions, 44 reported fewer than 10 taps for the year, including 19 who reported one tap and 36 who reported zero. The largest number of taps was reported by New York police, with 197 wiretaps installed [Wiretap Report 1992]. When FBI Director Louis Freeh lobbied Congress for the 1994 Communications Assistance for Law Enforcement Act (CALEA, better known as the "Wiretap Access Bill"), he cited FBI statistics claiming only 1,157 federal, state, and local electronic surveillance orders for all of 1993. To put these numbers into perspective, the FCC estimated that in 1993 the US had approximately 500 million phones covering 150 million phone numbers. Even the FBI itself seems unaware of any real problems in conducting wiretaps caused by encryption technology [Markoff 1994c]. The Wiretap Access Bill, S.2375, was passed with the unanimous consent of the senate, without any floor debate or reading of the bill, after a number of senators received a personal visit from FBI director Louis Freeh in the days before the vote [Bunker 1994] [Matthews 1994].

A view often advanced of the move towards increased surveillance and encryption regulation is that, with the end of the Cold War, a number of signals and intelligence agencies are experiencing difficulty justifying enormous budgets in the face of cutbacks in other areas of the ecomony (the US government spends more money — US$28 billion — on intelligence than it does on housing or education [Toledo 1995]. This budget was increased by 5% for 1996, a 1.3% increase over and above the requested amount). It appears that the various intelligence agencies may be moving from concerns over national security to concerns over job security, requiring a new mission to justify their budgets [Markoff 1994b]. For example, the Canadian Communications Security Establishment was recently criticised for carrying out economic espionage on Mexico during NAFTA talks and on Korea to facilitate the sale of Canadian nuclear reactors, with a former CSE employee admitting to CTV news that the CSE shifted its focus after the cold war from spying on the Russians to spying on Canadas allies and trading partners in order to acquire trade secrets [CP 1995].

In the face of strict encryption regulation or even the unlikely scenario of a complete ban on the use of any form of encryption, there still remains a means of communication which cannot be banned because it cannot be detected: steganography, the art of hiding one message inside another. Such techniques have been in use to keep communications secret for centuries, with the first known use being by the astronomer Aryabhata in around 500 AD, who used a technique which mapped numbers to letters which could yield cipher words which were meaningful text [Kak 1988]. More recently, the British War Office devised a steganographic protocol which allowed soldiers in WWII prisoner-of-war camps to communicate information in their letters despite intense scrutiny by prison camp guards [Rabson 1990]. To date the most common use of steganographic techniques is in the game of bridge, where its use to allow bridge partners to communicate secret information in direct view of their opponents has caused a certain amount of controversy [Winkler 1980a] [Winkler 1980b]. Due to the nature of the communications channel, the amount of information which can be transmitted via steganography is normally very limited (the WWII cipher would, for example, require an entire letter to conceal a few short phrases about enemy troop movements). However with the advent of essentially free computer communications this restriction on size is lifted — an expansion of a hundred to one for a simple message is no longer seen as a major problem, since at worst it will require a few seconds longer to transmit the “carrier” message, with the messy details of complex en- and decoding being taken care of by the computer. Communications by computer-aided steganography can take place through virtually any form of overt communication, with messages being hidden inside sound files, pictures, or text (typical methods involve inserting message bits into the least significant bits of graphical images or sound samples, or making minute changes in letter spacings in text). Because the hidden messages can be made arbitrarily difficult to detect by making them arbitrarily close to the expected characteristics of the carrier message, the result is an undetectable means of communicating in secret — a form of encryption which cannot be banned or outlawed. Software which implements various steganographic techniques is already

freely available, and has the potential to become widespread if more conventional means of securing data are outlawed.

5.The Market

The development of trading of goods and services in the Internet may drive the use of cryptography, and to some extent, force the hand of governments as to its use. As the market develops, larger sums of money will be circulated, and, presumably, criminal activity will upscale accordingly. Secure cryptography may be perceived as necessary to protect transactions, in the way that secure cryptographic protection for banks is already seen as valuable. Thus, the market may cause cryptography to lose the mystique of its traditional defence role, and it may be seen by consumers as another product of the information age that they wish to buy. It is likely that as consumers become more acquainted with the product, they will demand better services.

With encryption programs like PGP already in wide circulation outside the US, this development is likely to be rapid, and if the US holds on to its isolationist policy in regard to cryptography for too long, it may face the major economic risk of another nation producing high-quality cryptographic software, and setting a new standard outside the US. Such software is already being produced in countries outside the US. However, in the face of the US market dominance, and refusal to deregulate in the area of cryptography, it is likely the market will remain fragmented and without definitive standards for the forseeable future. It is likely that important attempts will be made by large multinational companies moving into the market to establish the technical standard of “adequate” cryptographic security, and to look towards the establishment of global standards.

6 Conclusion

The Internet backbone was set up with United States Government money and support, and the principle of an information superhighway is supported by the US Government. However, there is a strong impulse in the US and other countries to claw back political control over the Internet. Particularly problematic is the unprecedented scope of surveillance methods. These measures, being put in place possibly before the American people fully grasp the significance of them, may become the status quo, and difficult to shift in the future. However, in the area of cryptography, the US is facing a quiet rebellion on a number of fronts. One is the domestic resistance to the key forfeiture proposals and legislation which electronic civil rights activists believe will infringe individual privacy and freedom of Americans. The recent strong lobbying efforts by the Internet community in 1995 in respect of the Exon Communications Decency Act (where the Internet community believed legislation to control offensive material would damage the Net), and the resulting turnaround between the Senate passing the Communications Decency Act

legislation and the Congress passing the Cox-Wylie Amendment, (a more low-key and practical approach to the problem) would indicate the Internet community in America is rapidly learning to use its teeth. Another advance is the pragmatic arming of other countries with the weapons of future commerce, such as cryptography, securing of electronic communications against piracy and damage, and Internet access and literacy. These factors are likely to proceed to the point where the US technological supremacy may be under threat, and deregulation of cryptography will become unavoidable. Economic and defence adjustments would then have to be made. However, it is possible these may be more to the perceptions of Americans, rather than to the possibility that due to secure encrypted communications, the American economy may suffer disastrous damage, taxes will suddenly not be paid, the war against drugs will be lost completely, and bombers will run amok.

Governments of sovereign nations will each be in the position of deciding the trade-off between perceptions of security problems, protection of civil rights, and economic advantage. The cryptography issue may be seen as an issue of the relationship between government and citizens, with the Internet and cryptographic technology having the potential to substantially change the relationship. With complete privacy of transactions and the ability to dodge many traditional bureaucratic checks, a cryptography-based economy and society could cause governments to become shut out of many business and social transactions, unless people voluntarily allowed them in. The authors would argue that the new environment established by the Internet rightly demands a rethink of the social contract between governments and citizens, and that this contract must be viewed in its totality, as a contract involving issues of personal freedom and privacy, as well as governance. A power imbalance achieved by governments as a result of vastly increased ability to perform surveillance on citizens, may be seen as breaking the "collective enterprise" [Sharp 1984] which is the relationship of government to citizens. An ability by governments to accomodate the use of powerful encryption methods by citizens and negotiate on areas of law and order, crime, and so on, may be viewed as social progress by citizens. The process may represent the "coming of age" of the Internet.

The alternative is that an unprecedented, and undesirable, amount of power may come to reside in the government of countries, if key forfeiture cryptography schemes are introduced internationally. With its strong civil rights movement, the US Internet community has been well-placed to fight initiatives such as the Clipper Chip. That the Clipper Chip idea went as far as it did, is an indicator of how the rights of individuals in less democratic countries could be compromised if encryption "trapdoors" are built into national cryptographic systems, or if key forfeiture cryptographic systems were established and misused by national security agencies. The potential for human rights violations resulting from governments being able to gather "evidence" against dissidents on an unprecedented scale, is a major problem of new technology of surveillance being allied with cryptography regulation.

In general, cryptography policy may develop from commercial needs, privacy needs, and the need to protect societies. This last category should be generated by the

Internet itself. No one country can do it without imposing significant penalties. The potential of an ethical community of Internet users to control criminal activity, for example, is a good question for the Internet community to ponder. Many of the concerns of the Clipper architects are demonstrably real. Issues of encrypted criminal or terrorist transactions, and drug money laundering (with associated uncontrolled casino activity on the Internet) are issues that the Internet community should rightly address. However, these issues should be separated from the cryptography debate, and addressed as political issues for internet community members, rather than as problems addressed only by national law enforcement or defence agencies. If an issue thrown up by the debate is the relationship between governments and citizens, it is a worthy subject for the Internet community to study in terms of planning its own political future. If the Internet remains a politically anarchic system, it risks losing its community forum and its potential future as a global open information system to repression by national governments. In the climate of governments moving towards regulation to limit use of cryptography and to establish key forfeiture systems, it makes sense to look at the possibility of an Internet political movement as a protective device. Just as the US Association for Computing Machinery is calling for a major public study on the uses of encryption on the Internet, the Internet itself should be creating a major study field of this critical issue, and associated issues of criminal conduct using encryption. Existing Net organisations like the Web Society could have a major part in this.

A logical issue for the Internet community to address is that of effective cryptography standards for the conduct of business and personal communications. Public research into cryptography should be open, and the products of that research freely distributable without restriction.

A point to keep in focus when considering regulating security aspects of communications media like the networks used daily: a new technique for cryptography may appear in any moment which would foil any efforts to monitor or police the exchange of encrypted data. The potential of steganography, for example, sends a warning to governments which attempt to censor Internet communications through cryptography legislation. To demonstrate the difficulty in regulating (or even detecting) this means of communication, messages using each of the three steganography techniques mentioned above have been embedded in this paper.

Acknowledgements

The authors would like to thank Professor Bob Doran for helpful advice during the writing of this paper.

References

[AAAS 1984] "Project on Secrecy and Openness in Scientific and Technical Communications", American Association for the Advancement of Science, Committee on Scientific Freedom and Responsibility, Cryptologia Vol.8, No.2 (April 1984), p.109.

[ABCNY 1995] "The Clipper Chip: Should the Government Control the Master Keys to Electronic Commerce?", panel discussion sponsored by the Science and Law Committee and the Computer Law Committee of the Association of the Bar of the City of New York, 19 January 1995.

[ACE 1981] "Report of the Public Cryptography Study Group", American Council on Education, 7 February 1981.

[AHG 1995] "Aussenhandelsgesetz (AHG-EU)", 1 July 1995.

[Allen and Polmar 1988] Allen, T. and Polmar, N. "Merchants of Treason: America's Secrets for Sale, from the Pueblo to the Present", Dell Publishing, 1988.

[Anderson 1994a] Anderson, R. "Liability and Computer Security: Nine Principles", Proceedings of ESORICS'94, Springer-Verlag,1994.

[Anderson 1994b] Anderson, R. 17 June 1994, message-ID <2ts9a0$95r@lyra.csx.cam.ac.uk>, posted to sci.crypt newsgroup.

[Anderson 1994c] Anderson, R. Private communications.

[Anderson 1995] Anderson, R. "Crypto in Europe - Markets, Law, and Policy", Cambridge University Computer Laboratory, 1995.

[Arthur 1995] Arthur, C. "Internet's 30bn Pound Secret Revealed", UK Indpendent newspaper, 17 August 1995.

[Atkins et al 1994] Atkins, D., Graff, M., Lenstra,A., and Leyland, P. "The Magic Words are Squeamish Ossifrage", Advances in Cryptology - Asiacrypt'94 Proceedings, Springer-Verlag, 1994.

[Aviation Week 1995] "Military Gets Fastlane on Net", Aviation Week, 6 February 1995, p.47.

[Bamford 1982] Bamford, J. "The Puzzle Palace: Inside The National Security Agency, America's Most Secret Intelligence Organization", Penguin Books, 1982.

[Bank 1994] Bank, D. "The Keys to the Kingdom", San Jose Mercury News, 27 June 1994, p.1D.

[Barlow 1994] Barlow, J. "Jackboots on the Infobahn", Wired 2.04, April 1994.

[Barron 1987] Barron, J. "Breaking the Ring: The Bizarre Case of the Walker Family Spy Ring", Houghton Mifflin Co., 1987.

[Bigelow 1909] Bigelow, J. "Retrospections of an Active Life", New York, 1909.

[Blaze 1994] Blaze, M. "Protocol Failure in the Escrowed Encryption Standard", Proceedings of the 2nd ACM Conference on Computer and Communications Security, Fairfax, 1994.

[Bloodmoney 1992] "The Ultimate Cellular Modification Manual", 'Dr.Bloodmoney', 1 June 1992.

[Blum 1987] Blum, H. "I Pledge Allegiance… The True Story of the Walkers: An American Spy Family", Simon and Shuster, 1987.

[Bunker 1994] Bunker, T. "Is it 1984?", LAN Magazine, Vol.9, No.8 (August 1994).

[den Boer et al 1992] den Boer, B., Boly, J., Bosselaers, A., Brandt, J., Chaum, D., Damgård, I., Dichtl, M., Fumy, W., van der Ham, M., Jansen, C., Landrock, P., Preneel, B., Roelofsen, G., de Rooij, R., Vandewalle, J., "RIPE Integrity Primitives", ECRACE Document R1040, 1992.

[BorderWare 1995] "BorderWare Firewall Server Product Description", Border Network Technologies, 1995.

[Brod 1995] Brod, E. "This Is the CEO - Get Me the CIA", The Wall Street Journal, 14 November 1995, p.A15.

[Business Week 1995], Business Week, "The Bankers Trust Tapes", Department: Cover Story, October 16, 1995.

[CBC 1994] CBC Newsworld documentary on US satellite communication interception, 2 January 1994.

[CDT 1995a] "X9 to develop triple-DES standards", Centre for Democracy and Technology Policy Post No.2, 13 February 1995.

[CDT 1995b] "New Cryto Policy Flops at Conference", Center for Democracy and Technology Policy Post No.24, 11 September 1995.

[CEI 1992] "SuperCrypt CE99C003A Technical Reference (Preliminary)", CE Infosys, Germany, 1992.

[Chaum 1992] Chaum, D. "Achieving Electronic Privacy", Scientific American, August 1992, pp 96-101.

[CFP 1994] "Data Encryption: Who Holds the Keys?", Panel discussion at the Fourth Conference on Computers, Freedom and Privacy, Chicago, Illinois, 24 March 1994.

[CIA 1994] Central Intelligence Agency, "A Consumer's Guide to Intelligence", 12 April 1994.

[Clarke 1992] Clarke, R. "Just Trade? A Seminar on Unauthorised Release of Government Information", Australian National University, 12 October 1992.

[Collins 1995] Collins, L. "Bulk RC4 brute forcing", 2 Dec 1995, message-ID: <199512030356.OAA17497@oznet02.ozemail.com.au>, posted to the cypherpunks mailing list.

[Corcoran 1995] Corcoran, E. "Encryption Control Plan Sparks Industry Protest: High-Tech Groups Say Proposals Unworkable", The Washington Post, 8 November 1995.

[CP 1995] "Electronic snooping part of the game", CP Canadian News Digest, 15 November 1995.

[CSE 1993] "Statement of Work For the Research and Development of A Topic Spotting System", (Canadian) Communications Security Establishment Contract W2213-3-1903, Annex B, March 1993, p. 11.

[Cryptech 1989] "The CRY12C102 DES CHIP Technical Reference Manual", Cryptech NV/SA, Brussels, 1989.

[Davida 1981] Davida, G. "The Case Against Restraints on Non-Governmental Research in Cryptography", Cryptologia Vol.5, No.3 (July 1981), p.143..

[Deavours 1986] Deavours, C. "Elle a de l'intelligence et de la conversation", Cryptologia Vol.10, No.1, January 1986.

[Deavours 1987] Deavours, C. "Sois Belle te Tais-Toi", Cryptologia Vol.11, No.3 (July 1987), p.162.

[Deeley 1985] Deeley, W. (NSA Director for Communications Security) Testimony to the House Committee on Science and Technology, June 1985.

[Department of Commerce 1980] Department of Commerce, "White Paper of National Security Policy Options for Cryptography", National Communications and Information Administration, 17 November 1980.

[Department of State 1989] Department of State, "International Traffic in Arms Regulations", 22 CFR 120-130, Office of Munitions Control, November 1989.

[Department of State 1992] Department of State, "Defense Trade Regulations", 22 CFR 120-130, Office of Defense Trade Controls, May 1992.

[DISSI 1995] DISSI, "Autorisation de fourniture et d'utilisation generale de moyens de cryptologie No. 2500", 509/DISSI dossier numero 950038, 7 November 1995

[Dubner and Dubner 1992] Dubner, R. and Dubner, H. "A Proposal For Making High-Speed Numerical Calculation Economically Available to Wide Range of Researchers", 12 April 1992.

[ECPA 1988] Electronic Communications Privacy Act, 9 March 1988.

[Ellison 1995] Ellison, C. "How long would an escrow system survive", 30 May 1995, message-ID <3qe8n7$cmo@clark.net>, posted to the alt.security.pgp newsgroup.

[Elmer-Dewitt 1994] Elmer-Dewitt, P. "Who Should Keep the Keys?", Time Magazine, 14 March 1994.

[EPIC 1995] Electronic Privacy Information Center (EPIC) Alert, Vol.2.09, 21 August 1995.

[EU 1995] "EU Directive on Export Control (COM 837 (95)", 10 April 1995.

[FBI 1993] "Encryption: The Threat, Applications, and Potential Solutions", declassified FBI, NSA, and DOJ briefing document sent to the National Security Council in February 1993.

[FBI Undated a] "Impact of Emerging Telecommunications Technologies on Law Enforcement", declassified FBI report, undated.

[FBI Undated b] "Telecommunications Overview", Advanced Telephony Unit, declassified FBI presentation on encryption policy, undated.

[Federal Register 1992] "Proposed Reaffirmation of Federal Information Processing Standard 46-1, Data Encryption Standard", Federal Register, Vol.57, No.177 (11 September 1992),p.41727.

[Federal Register 1995] Federal Register, 16 October 1995 (Vol.60, No.199), p.53,643.

[FIfF 1995] "Abhörbefugnisse nach Plan", Presseerklärung des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V, Bonn, 14 December 1995.

[Fox 1995] Fox, D. "Lauschordnung",c't, July 1995.

[Froomkin 1995] Froomkin, M. "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution", 143 U.Penn Law Review 709, 1995.

[Garfinkel 1995] Garfinkel, S. "PGP: Pretty Good Privacy", O'Reilly and Associates, 1995.

[Gilbert 1981] Gilbert, L. "Patent Secrecy Orders: The Unconstitutionality of Interference in Civilian Cryptography", L.Gilbert, Santa Clara Law Review, Vol.22 (1981), p.325.

[Griffin 1995] Griffin, J. "Pakistan Forces Motorola To Halt Cellular Services In Karachi", Voice of America, 4 March 1995.

[Harris 1994] Assistant Attorney General Jo Ann Harris, testimony to Senate Judiciary Subcommittee, 3 May 1994.

[Hellman 1993] Reported by Martin Hellman at the 1993 RSA Data Security Conference, 14-15 January 1993.

[Hoffman 1995] Hoffman, L. "Building in Big Brother: The Cryptographic Policy Debate", Springer-Verlag, 1995.

[Internet 1995] http://www.poptel.org.uk/labour-party/

[ISO 1987] ISO 8372:1987, "Information Processing - Modes of operation for a 64-bit block cipher algorithm", 1987.

[ISO 1988a] ISO 8730:1988, "Banking - Requirements for Message authentication", 1988.

[ISO 1988b] ISO 8732:1988, "Banking - Key Management (Wholesale)", 1988.

[ISO 1991a] ISO 10116:1991, "Information Technology - Modes of operation for an *n*-bit block cipher", 1991.

[ISO 1991b] ISO 10126:1991, "Banking - Procedures for message encipherment (Wholesale)", 1991.

[James 1995] James, D. "The Application of Classical Information Retrieval Techniques to Spoken Documents", PhD thesis, Downing College, UK, 1995.

[Johnson 1995] Johnson, J. "Info'Hypeway": A Worst Case Scenario". Address, ACM Conference on Computer-Human Interaction, 1995.

[Kak 1988] Kak, S. "The Aryabhata Cipher", Cryptologia Vol.12, No.2 (April 1988), p.113.

[Knapp 1993] Letter from Michael F. Knapp, Inspector-Deputy Chief, Office of Public and Congressional Affairs, 16 July 1993.

[Kolata 1986] Kolata, G. “NSA to Provide Secret Codes”, Science Magazine, 4 October 1986.

[Kruh 1986a] Kruh, Louis, "The Control of Public Cryptgraphy and Freedom of Speech - A Review", Cryptologia Vol.10, No.1 (January 1986), p.2.

[Kruh 1986b] Kruh, L. “Cryptology and the Law - VII”, Cryptologia Vol.10, No.4 (October 1986), p.248.

[LA Times 1994] “Column One”, LA Times, 3 October 1994.

[Lagan and Davies 1993] Lagan, B., and Davies, A. “New digital phones on line despite objections”, The Sydney Morning Herald, Wednesday 28pril, 1993.

[Lees 1995] Lees, D. Response to a written query about encryption policy, David Lees, Adminsitration Officer to Rt. Hon. Paddy Ashdown MP.

[Lenstra and Lenstra 1993] Lenstra, A., Lenstra, H. Jr., “The development of the number field sieve”, Lecture Notes in Mathematics 1554, Springer-Verlag, 1993.

[Levy 1993] Levy, S. “Crypto Rebels”, Wired, May 1993.

[Lloyd 1993] Lloyd, C. “Spymasters Order Redesign of ‘Too Secure’ Mobile Phones”, The Sunday Times, 31 January 1993, p.12.

[Lomas 1994] Lomas, T., and Roe, M. “Forging a Clipper Message”, Communications of the ACM Vol.37, No.12 (December 1994), p.12.

[Luck and Burns 1994] Luck, N. and Burns, J. “Your Secrets for Sale”, Daily Express, 16th February 1994, p.32.

[Madsen 1993a] Madsen, W. “NCIC Criticised for Open Security and Privacy Doors”, Computer Fraud and Security Bulletin, October 1993, p.6.

[Madsen 1993b] Madsen, W. “The Inslaw Affair”, Computer Fraud and Security Bulletin, September 1993, p.12.

[Madsen 1994] Madsen, W. “Norwegian encryption standard moves forward”, Computer Fraud and Security Bulletin, November 1994, p.10.

[Markoff 1992] Markoff, J. “A Public Battle Over Secret Codes”, The New York Times, 7 May 1992.

[Markoff 1994a] Markoff, J. “Scientist Insists U.S. Computer Chip has Big Flaw”, Detroit Free Press, 2 June 1994.

[Markoff 1994b] Markoff, J. “A Push for Surveillance Software”, New York Times, 28 February 1994.

[Markoff 1994c] Markoff, J. “U.S. Code Agency is Jostling for Civilian Turf”, New York Times, 24 January 1994.

[Markoff 1995a] Markoff, J. “F.B.I. Proposes Huge Wiretapping System”, The New York Times, 2 November 1995.

[Markoff 1995b] Markoff, J. “Industry Group Rebuffs U.S. On Encryption”, The New York Times, 8 November 1995.

[Markt & Technik 1994] “Zweifelhafter Datenschutz”, “Markt & Technik - Wochenzeitung für Elektronik” Nr. 18, 29 April 1994, p.49, .

[Matthews 1994] Matthews, C. “Unanimous Nod For Wiretap Bill”, “The Spotlight”, Technology & Liberty, 7 November 1994.

[Matthews 1995] Matthews, C. “Administration Plans 1.5 million Telephone Intercepts”, “The Spotlight”, Technology & Liberty, 13 November 1995.

[McLeod 1993] McLeod, K. “Covert Local Area Network Surveillance”, Computer Audit Update, October 1993, p.13..

[McPartlin 1993] McPartlin, J. “GAO: FBI Breach is an Inside Job”, Information Week, 9 September 1993.

[Meeks 1995] Meeks, B. “Target: Internet”, Communications of the ACM, Vol.38, No.8 (August 1995), p.23.

[Mercury News 1993] San Jose Mercury News, 24 August 1993.

[Merkle 1991] Merkle, R. “Fast Software Encryption Functions”, Advances in Cryptology - Crypto’90 Proceedings, 1991,p.476.

[Moscow Times 1995] Moscow Times, “FAPSI given worrying new powers”, 4th May 1995.

[Motorola 1993] Motorola Cellular Subscriber Technical Training Manual, July 1993, Item #68P09300A60-C.

[Murray 1993] Murray, W. 20 August 1993, message-ID: <930820201552.103567@DOCKMASTER.NCSC.MIL>, posted to the sci.crypt newsgroup.

[NAP 1991] "Finding common ground: U.S. export controls in a changed global environment", National Academy Press, Washington, D.C., 1991.

[NCSA 1995] NCSA HTTPD version 1.4.1 buglist.

[NIST 1995] "Discussion Paper #4", NIST Key Escrow Issues Meeting, 6 September 1995.

[Orlowski 1995] Orlowski, S. "Encryption and the Global Information Infrastructure: An Australian Perspective", presented at the Cryptography Policy and Algorithms Conference, Queensland University of Technology, July 1995.

[OTA 1987] "Defending Secrets, Sharing Data: New Locks and Keys for Electronic Communications", Office of Technology Assessment OTA-CIT-310, October 1987.

[PC Week 1993] "DES Killer Ensures Secure Government", PC Week Magazine, 20 October 1993.

[Pierce 1984] Pierce, K. "Public Cryptography, Arms Export Controls, and the First Amendment", Cornell International Law Journal, Vol.17, No.1 (Winter 1984), p.197.

[Polmar and Allen 1989] Polmar, N. and Thomas Allen, T. "The Crypto Bandits", Air Force magazine, June 1989, p.88.

[Price 1989] Price, W. "Standards for Data Security", published in "Cryptography and Coding", Beker, H, and Piper, F. (editors), Clarendon Press, 1989.

[Quittner 1994] Quittner, J. "U.S.Nears Standard on Coding Messages", Newsday, 8 June 1994.

[Rabson 1990] Rabson, J., and Rabson, H. "The War Office HK POW Cipher System", Cryptologia, Vol.14, No.7 (January 1990), p.53.

[Rainville 1994] Rainville, J. "NSA Reasons for Negative Vote", 7 November 1994.

[Relyea 1994] "Silencing science: National security controls and scientific communication", Ablex Publishers, Norwood, NJ, c1994.

[Remijn 1994] Remijn, M. "Tekst van de memorie van toelichting van de wet tegen crypto", 15 April 1994, message-

ID<1994Apr15.124341.20420@news.research.ptt.nl>, posted to the nlnet.cryptographie newsgroup.

[Reuters 1994] Reuters, "US Spied on British Defence Projects", London, 5 October 1994.

[Risks 1993] ACM RISKS-Forum Digest, Vol.14, Issue 34, 22 Feb 1993.

[Roberts 1988] "Technology transfer: A policy model", National Defense University Press, Washington, DC, 1988.

[Root 1991] Root, W. "United States export controls, 3rd ed", Prentice Hall Law & Business, Englewood Cliffs, NJ 1991.

[Rossiyskaya Gazeta 1995] Rossiyskaya Gazeta, #68, 6 April 1995.

[Safire 1994] Safire, W. "Sink the Clipper Chip", New York Times, 14 February 1994.

[Sandberg 1995] Sandberg, J. "French Hacker Cracks Netscape Code, Shrugging Off U.S. Encryption Scheme", The Wall Street Journal, 17 August 1995, p. B3.

[Schroeder 1995] Schroeder, B. "Schnueffler am Ende: Datenverschluesselung - Bonn muss die Fakten erkennen", Die Zeit, No.37, 1995.

[Sharp 1984] Sharp, A. "Pride, Resentment and Change in the State and the Economy. Leap Into The Dark, The Changing Role of The State In New Zealand Since 1984", p.225-249.

[Smid and Branstead 1988] Smid, M. and D.Branstead, D. "The Data Encryption Standard: Past, Present, and Future", Proceedings of the IEEE, Vol.76, No.5 (May 1988), p.550.

[Spiegel 1996] "Der Spiegel", Ausgabe 02/96, 8 January 1996, p.106.

[taz 1995] "Wie eine Spinne im Netz", Die Tageszeitung (taz), 26 June 1995.

[Toledo 1995] Toledo, R. "Secret Spying Budget Tops $28 billion", NY Transfer News Collective, 1995.

[USA Today 1995] Editorial, USA Today, 25 October 1995.

[Walker 1994] Walker, S. "An International Cryptographic Experiment: A Solution to the International Use of Cryptography?", Trusted Information Systems Report #521, 12 April 1994.

[Wilder and Violino 1995] Wilder, C., and Violino, B. "CyberTheft Threatens New Frontier", Infotech Weekly, 4 September 1995, p.10.

[Winkler 1980a] Winkler, P. "Encrypted Signalling", "The Bridge World", April 1980, p.25.

[Winkler 1980b] Winkler, P. "Cryptologic Techniques in Bidding and Defense", Parts I - IV, Bridge Magazine April-July 1980.

[Wiretap Report 1992] "Report on applications for orders authorizing or approving the interception of wire, oral, or electronic communications" (more commonly known as the "Wiretap report"), Statistical Analysis and Reports Division, Administrative Office of the U.S. Courts, 1992.

[X9 1994] "ASC X9 Project Proposal", X9 New Work Item Proposal, 27 July 1994.