PREPARED STATEMENT OF PHILIP R. KARN, JR., STAFF ENGINEER, QUALCOMM, INC.

Security and Freedom Through Encryption (SAFE) Act
March 20, 1997 - House Judiciary Subcommittee on Courts and Intellectual Property

Dear Mr. Chairman, thank you for the opportunity to appear before your Committee in support of H.R. 695, the *Security and Freedom through Encryption (SAFE) Act.* I am pleased to submit this written testimony with additional details about my case and pointers to more information on encryption, its worldwide availability, and the effects that the current export control regime have on the security and privacy of US citizens. This document is available on the Internet as http://www.qualcomm.com/people/pkarn/export/housewritten.html.

In that form it contains many links to related information on the Internet.

I maintain a comprehensive Internet archive of the *Applied Cryptography* case, including all my correspondence with the State Department and the briefs of both sides in our lawsuit. The URL is http://www.qualcomm.com/people/pkarn/exportl.

THE ''APPLIED CRYPTOGRAPHY'' CASE

The book *Applied Cryptography* by Bruce Schneier that is the subject of my case was first published in early 1994. Mr. Schneier estimates that the first edition sold 30,800 copies. The second edition, published in 1996, has sold 34,300 copies in the US. Another 15% have been sold internationally; there are translations into French (3,000 copies), German (2,000) and Polish. It is now being translated into Japanese and Spanish.

Mr. Schneier's publisher, John Wiley and Sons, has kindly contributed a dozen copies of his book to the Committee. I consider it an excellent reference on modern cryptography and I hope the Members and their staffs will find it useful in understanding the subject. I should state that I have no connection to Mr. Schneier other than as a satisfied reader. Although I did contribute minor material to the book, I have no financial interest in its sales.

Applied Cryptography is a comprehensive book, but it is by no means unique in having source code listings of strong encryption algorithms (ciphers). Many other textbooks on cryptography describe ciphers such as the US Data Encryption Standard (DES) in complete detail, and some include source code. Computer magazines with

worldwide circulation such as *Byte and Dr. Dobbs Journal* (DDJ) have featured source code listings of ciphers such as DES, IDEA (used in *Pretty Good Privacy*) and the like. DDJ specializes in articles for programmers that contain source code; Mr. Schneier is a frequent contributor to that magazine. They have long made all of their source code listings available on CD–ROM and over the Internet.

Computer books and magazines frequently print source code to illuminate the discussion of an algorithm in the accompanying text. The English language, or any natural language for that matter, is notoriously ill-suited to describe computer algorithms. Computer programming languages are designed not only for compilation by a computer into machine code for eventual execution, but also to communicate an algorithm in a concise, unambiguous way to a skilled human reader. As the preface to a computer science textbook stated:

Our design of this introductory computer-science subject reflects two major concerns. First, we want to establish the idea that a computer language is not just a way of getting a computer to perform operations but rather that it is a novel formal medium for expressing ideas about methodology. Thus, programs must be written for people to read, and only incidentally for machines to execute. (H. Abelson and G. Sussman, *Structure and Interpretation of Computer Programs,* MIT Press 1985.)

The source code in *Applied Cryptography* follows that philosophy. In a ruling in the related case of *Bernstein* vs. *Department of State* US District Judge Marilyn Hall Patel specifically held that source code is protected speech under the First Amendment:

Defendants appear to insist that the higher the utility value of speech the less like speech it is. An extension of that argument assumes that once language allows one to actually do something, like play music or make lasagne, the language is no longer speech. The logic of this proposition is dubious at best. Its support in First Amendment law is nonexistent.
For the purposes of First Amendment analysis, this court finds that source code is speech. (Opinion, Docket C–95–0582 MHP, April 15, 1996).

Yet the government totally ignored this and Judge Patel's subsequent ruling on December 6, 1996 holding that the 1TAR as applied to encryption source code was a

violation of the First Amendment. They continue to treat this information as a dangerous weapon. Indeed, on December 30, 1996 they dug their heels in deeper: A printed book or other printed material setting forth encryption source code is not itself subject to the EAR (see Sec. 734.3(b)(2)). However, notwithstanding Sec. 734.3(b)(2), encryption source code in electronic form or media (e.g., computer diskette or CD ROM) remains subject to the EAR (see Sec. 734.3(b)(3)). The administration continues to review whether and to what extent scannable encryption source or object code in printed form should be subject to the EAR and reserves the option to impose export controls on such software for national security and foreign policy reasons. (Department of Commerce, Bureau of Export Regulation, *Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, Federal Register,* December 30, 1996, pp. 68572–68587).

This is from an ''interim rule'' transferring jurisdiction over civilian encryption items from the International Traffic in Arms Regulations (ITARs) administered by the State Department to the Commerce Control List (CCL) administered by the Bureau of Export Administration (BXA) in the Commerce Department. The new rules provide no substantive relief over the old rules. Indeed it is hard to understand why the Administration went to the trouble of making the change except as a cynical attempt to ''respond'' to the sustained public protests against US encryption policy by injecting further uncertainty and confusion. Perhaps they just got tired of us holding up our floppy disks and proclaiming that the US Government considers them ''munitions.'' Now they're merely ''encryption items,'' but I could still go to jail for exporting one.

One effect of the transfer was an additional delay in processing licensing applications. Our export department at Qualcomm reports that one license application had been pending at State for 42 days when the new rules were issued. State then returned the application without action. It took another 42 days to finally obtain approval from Commerce. Our export administrator does report that the paperwork requirements with Commerce are somewhat less onerous than with State.

The lengths to which the government appears willing to go to suppress readily available cryptographic software are truly remarkable. Indeed, it seems to be an even bigger threat than nuclear weapons information. Consider the 1979 case of *US* vs. *The Progressive,* where the government tried to suppress an article on the

principles of nuclear weapons based wholly on public information. The government predicted all sorts of dire consequences should this information be published. But the article appeared anyway in the US press. Once this happened, the government dropped its case. It did not then try to stop it at the borders because that was obviously impossible, even without a global Internet. Yet that is precisely what they are trying to do with encryption software. As the *Los Angeles Times* said recently in an editorial, the encryption horse has not only left the barn, it has been on a worldwide tour.

THE AVAILABILITY OF ENCRYPTION SOFTWARE ON THE INTERNET

The *Applied Cryptography* source code is readily available on the Internet from a site in Italy (ftp://idea.dsi.unimi.it//pub/security/crypt/applied-crypto/). Countless other Internet sites around the world also have encryption software. Some are subroutine libraries like those in *Applied Cryptography* that are only of use to programmers who can incorporate them into complete applications.

Others packages are complete applications that can be installed and run by the end user. The well-known Pretty Good Privacy (PGP) package is only one example. Another more recent package with which I am familiar is the Secure Shell (SSH) by Tatu Ylonen of Finland. While PGP is primarily suited to electronic mail, SSH provides highly secure remote access, file transfer and command execution between Unix, Windows-95 and Macintosh operating systems. SSH provides a choice of strong ciphers, including ''triple DES.'' Several years ago, the American National Standards Institute (ANSI) standardized triple DES at the request of the banking industry—over the strenuous objections of the National Security Agency. Needless to say, SSH does not provide key escrow.

Mr. Ylonen has made the full source code of his software freely available on the Internet where in just two years it has become a de-facto standard. This shows how the foreign competition to the US software industry is not limited to large companies. One suitably motivated and talented individual, living in a country without export controls, can produce strong, unescrowed encryption software and have it rapidly adopted by the Internet community. Because Mr. Ylonen has encouraged free copying of his software he does not know precisely how many use it. He estimates that several tens of thousands of organizations and hundreds of thousands of individuals—perhaps as many as a million—use SSH.

THE EFFECT OF EXPORT CONTROLS ON CELLULAR TELEPHONY

As I stated in my prepared remarks, export controls on cryptography have prevented the use of strong, well-studied ciphers in the new crop of digital cellular telephone systems now being deployed in the US. The industry has instead pursued weak ciphers that can pass export muster. At first the industry tried to keep their designs confidential, out of concerns over export law and also to hide their weaknesses.

Now it turns out that these weaknesses are even worse than was thought. The new paper *Cryptanalysis of the Cellular Message Encryption Algorithm* by David Wagner, a graduate student at the University of California, Berkeley, and Bruce Schneier and John Kelsey of Counterpane Systems describes how to break this cipher:

This paper analyzes the Telecommunications Industry Association's Cellular Message Encryption Algorithm (CMEA), which is used for confidentiality of the control channel in the most recent American digital cellular telephony systems. We describe an attack on CMEA which requires 40—80 known plaintexts, has time complexity about 2^{24}–2^{32}, and finishes in minutes or hours of computation on a standard workstation. This demonstrates that CMEA is deeply flawed.

The paper concludes as follows:

Our cryptanalysts of CMEA underscores the need for an open cryptographic review process. Betting on new algorithms is always dangerous, and closed-door design and proprietary standards are not conducive to the best odds.

The attack described in this paper is practical, and can be used against existing cellphones that use CMEA for security. CMEA is deeply flawed, and should be carefully reconsidered.

Again, the closed-door design process was largely the result of concerns over export controls. The industry was concerned that even publishing their ciphers for review might violate the law. This deprived them of the benefits of free and open scientific inquiry.

I wish to emphasize that the new digital cellular systems are still *much* harder to intercept than the sting analog (AMPS) systems like that used by Speaker Gingrich in his now-famous phone call. But they are not nearly as secure as they could have been. While industry politics and public apathy were also to blame, export controls were clearly the major culprit.

COMMENTS ON THE PROPOSED LEGISLATION

The proposed legislation, H.R. 695, the *Security and Freedom through Encryption (SAFE) Act,* is a big step toward restoring common sense and reason to our encryption policy. I am especially gratified that it would completely deregulate the export of publicly available encryption software such as the *Applied Cryptography* code so that it can be used as easily by the ''good guys'' as well as the bad guys who already have it.

My main concern with the legislation as written deals with the provisions that allow the Secretary of Commerce to determine whether there is ''substantial evidence'' that encryption software will be diverted to terrorist or hostile military use, or whether ''comparable'' cryptographic hardware is available from foreign suppliers. Past experience with the existing export laws shows that such provisions are ripe for abuse by the Executive branch. They should be backed up with explicit provisions for judicial review, and the full provisions of the Administrative Procedures Act (APA) should apply.

I am also concerned with the provisions that would create a new federal crime of using encryption in the commission of a crime. This may well have the effect of making a federal case out of even a minor criminal offense because of the incidental use of a device that happens to include encryption-like functions, such as a digital cordless phone. I believe this provision, if it is retained at all, should be more carefully tailored to the deliberate use of encryption to substantially impair the investigation of a major federal crime. The states would still be free to establish similar statutes for state offenses.

Dear Mr. Chairman, I offer these supplemental remarks for the record following my appearance before your committee on March 20, 1997 in support of H.R. 695, the *Security and Freedom through Encryption (SAFE) Act.*

I would like to respond to the Government witnesses on the first panel. Their

testimony included numerous inaccurate and/or misleading statements. I have heard and rebutted many of these claims in my court case, and I would like to do the same in this forum.

CONTRARY TO THE GOVERNMENT'S CLAIMS, A THRIVING CIVILIAN KEY MANAGEMENT INFRASTRUCTURE ALREADY EXISTS

The government witnesses go on at great length about the need for what they call a ''key management infrastructure'' (KMI) to authenticate public encryption keys. See, for example, pages 3–7 of Mr. Crowell's written statement.

This much is true. But on page 7 Mr. Crowell claims, incredibly,

An encryption support infrastructure does not exist today, other than in the KMI used by the Defense Department and other specialized areas....

See also Mr. Litt's statement on page 13:

... there is not yet an infrastructure to support the distribution of keys among users ... Such an infrastructure will have to be created ....

These statements are simply false. It is particularly difficult to understand how Mr. Crowell, whose agency's mission certainly includes staying abreast of civilian developments in cryptography, could be so misinformed.

The civilian crypto community is well aware of the need to authenticate public keys. The basic principles are documented at length in *Applied Cryptography.* Much of the code in a typical encryption software package (e.g., *Pretty Good Privacy,* PGP) is devoted to this one issue. And a viable and rapidly growing commercial Key Management Infrastructure now exists. Two complementary KMIs, in fact: the hierarchical KMI used for secure World Wide Web transactions, among other things, and the distributed ''KMI'' introduced by PGP. Each has its advantages.

The government may quibble that these KMIs don't ''count'' because they don't meet their precise definition of a KMI. For example, contrary to the second item of the list on page 5 of Mr. Crowell's statement, a KMI need *not* (and should not) generate or store user private keys. Such practices constitute an unnecessary security risk. Key pairs are best generated by the end user's device, and only the public component of the key pair need ever leave the device.

If the DoD's KMIs for classified information do generate and store all their private keys in a central location where they can be stolen en masse by some future Aldrich Ames, then I submit that Mr. Crowell's agency is seriously remiss in its duty to provide the best possible protection for secret US Government data. Also keep in mind that several spy scandals, such as the Walker/Whitworth case of the mid 1980s, involved the compromise of cryptographic keys for remarkably small sums.

True, Mr. Crowell did not actually say that the DoD KMI he mentions is used to secure classified data, though he might have meant us to make that inference. Indeed, other NSA employees have reportedly said that key recovery is not incorporated into encryption systems approved for classified data ''because of the obvious risks.'' Such statements speak volumes about the government's sincerity in supporting strong encryption for the law-abiding.

What counts about the civilian KMIs is that individuals and commercial entities do trust them for sensitive communications and commerce. For the government to say otherwise, to imply that only they have the expertise to make encryption safe for commerce, and to imply that a KMI must also generate and escrow secret keys so that public keys can be trustworthy, seems like a deliberate and cynical attempt to mislead Congress.

For example, several banks already rely on the encryption in web browsers such as *Netscape Navigator and Microsoft Internet Explorer* to protect transactions with their customers. Each bank has a public key certified by a ''certificate authority'' (CA) that attests to its authenticity. When the customer connects to the bank's web site, the user's web browser automatically verifies the bank's certificate. The customer can then conduct business knowing that he or she is actually talking to the bank's computer and not to some hacker's computer impersonating the bank.

The CAs follow strict safeguards including secured rooms and tamper-resistant hardware. There are already ten commercial CAs listed in the Security Options page of the *Netscape Navigator* browser. Some are established companies, such as BBN, AT&T, GTE and MCI; others, such as Verisign, are small entities that specialize in this service. One is even a governmental entity: the United States Postal Service.

Internet banks include Bank of America and Wells Fargo. The latter even lets customers write checks to arbitrary recipients, provided that the customer use the non-exportable (strong encryption) version of *Netscape Navigator* for this particularly sensitive function. Clearly they have more trust in this ''nonexistent'' KMI

than in the strongest encryption software the government will allow to be exported.

The other type of KMI is the distributed scheme embodied in PGP, where there are no formal CAs. *Everyone* can sign a key, but no one is required to honor the signature. One may trust only those keys he or she has personally signed, or one may also rely on signatures made by other persons whose competence and integrity in key signing he trusts. The important thing is that the user sets his own policy on key acceptance, while in the hierarchical scheme everyone is forced to trust the CA.

PGP ''key signing parties'' are now common at large physical gatherings of Internet users. Each attendee identifies him or herself to the others' satisfaction, usually by exchanging drivers licenses, passports and personal introductions. The attendee then reads his or her public key (actually a ''fingerprint'' of this key) so that the others may verify its correctness and later sign that particular key.

CONTRARY TO THE GOVERNMENT'S CLAIMS, SOFTWARE ON THE INTERNET IS NOT INHERENTLY UNTRUSTWORTHY

This specious claim has been made in my case against the State Department. Mr. Litt makes it again on page 13 of his statement:

Finally, the vast majority of businesses and individuals with a serious need for strong encryption do not and will not rely on encryption downloaded from the Internet from untested sources, but prefer to deal with known and reliable suppliers.

Mr. Litt is apparently unaware that Internet downloading is already the preferred way to obtain PGP, SSH, Netscape Navigator and other popular encryption software packages.

Aside from this fact, his argument does not withstand scrutiny for two reasons:

First, much encryption software is posted to the Internet in source code form. It can be verified by anyone who cares to read it. For example, the source code to *Applied Cryptography* on the Internet site in Italy can be visually compared against the listings printed in the book. The same is true for the PGP source, which has also been published in book form.

The user can write a test program to compare the results of encrypting a given ''test vector'' with a result known in advance, and so forth. Even if most users lack the skill or the time to perform these tests themselves, experience shows that if a problem exists in a widely used piece of software, sooner or later someone will discover it and

announce it widely on the Internet.

Open publication of encryption software not only makes it very difficult to conceal a deliberate flaw, it also facilitates the discovery of accidental flaws. The flaws in the Cellular Message Encryption Algorithm that were described by Wagner et al certainly would have come to light sooner had it been openly published on the Internet. Clearly the cellular industry didn't do very well by relying on a ''known and reliable supplier'' that wasn't willing to openly publish its work.

Security flaws in software available on the Internet are often discovered by the public even when the relevant source code is not generally available. The best examples are the various security-related Web browser bugs that are occasionally discovered and announced, usually by college students. In these cases the discoverers were not deterred by having to reverse engineer enough of the program to detect the flaw.

Second, it is already common practice to cryptographically ''sign'' software distributions on the Internet to guard against malicious creation and/or modification. PGP is widely used for this purpose, not only for cryptographic software such as SSH (from Finland) and PGP itself, but for other software such as operating system patches and updates, particularly those with security implications. While this practice does not guarantee that the software is completely secure, it does eliminate an entire class of potential attacks.

While no one can ever say that a particular piece of software is absolutely secure just as no one can say with certainty that it has no bugs, open publication and cryptographic authentication have made the distribution of software on the Internet in practice no more risky than its distribution by other means, such as floppy disks in retail stores (which are also not invulnerable to tampering.)

LAW ENFORCEMENT HAS MANY ALTERNATIVES

The government would have us believe that strong encryption will completely thwart the prosecution of many serious crimes. When pressed, they will cite a few anecdotes. For example, on page 4 of his statement Mr. Litt mentions the Aldrich Ames and Ramzi Yousef cases, asserting that both subjects used encryption to hide evidence of their crimes. He didn't say that both were easily convicted on the basis of other overwhelming evidence. Indeed, Mr. Ames pleaded guilty.

Mr. Ames' case is especially illustrative, as much of the evidence against him apparently came from microphones physically planted in his house that picked up

many incriminating telephone conversations. Even if Mr. Ames had been using an unbreakable encrypting telephone for these conversations the bugs would have heard his side of the conversation just fine.

One would not know it from Mr. Litt's dire warnings, but wiretaps are not their sole investigative tool. The alternatives include audio bugs (as in the Ames case), visual surveillance, undercover infiltration, informants (''moles''), testimony of collaborators compelled through grants of immunity, information from cooperating witnesses and institutions (e.g., bank records), physical and forensic evidence, and the like. Strong encryption has no effect whatsoever on these methods. In fact, its widespread use could actually *enhance* them, e.g., by allowing an undercover officer or informant to communicate securely with law enforcement without raising the suspicions of the subjects of the investigation.

Perhaps they do not discuss these alternatives out of fear of compromising their effectiveness. Personally, I think they simply don't want to say anything that might weaken their argument.

Mr. Litt's citation on page 5 of a computer hacker who used encryption is particularly vexing. While encryption is only one tool for keeping hackers out of computers, it is a vital one. It is ironic that he would complain about a hacker using encryption to hide the evidence of his exploits while supporting export controls that limit our ability to stop these attacks in the first place.

THE FOURTH AMENDMENT DOES NOT ''GUARANTEE'' GOVERNMENT ACCESS

The government would have us believe that the Fourth Amendment to the Constitution somehow entitles them to a successful search. Nothing could be further from the truth.

This is a classic example of the danger Alexander Hamilton warned us about in Federalist No. 84:

I go further, and affirm that bills of rights, in the sense and to the extent in which they are contended for, are not only unnecessary in the proposed Constitution, but would even be dangerous. They would contain various exceptions to powers not granted; and, on this very account, would afford a colorable pretext to claim more than were granted. For why declare that things shall not be done which there is no power to do?

This is precisely what has happened here. Over Hamilton's objections, the Bill of Rights was added to the Constitution solely to limit the power of government. Now the government perversely reads the Fourth Amendment as guaranteeing a *successful* search.

Indeed, if one also looks at the Fifth Amendment, the Founding Fathers were adamant that a suspect could not be compelled to give information that aids his own prosecution, no matter how useful that information may be. Yet that is precisely what the government wants through ''key recovery''—they want everyone, by their Hobson's choice of a key recovery system, to aid in their possible prosecution at a future date. Perhaps even the government recognizes the clear Constitutional implications of this philosophy, which is why they have not yet dared to propose mandatory domestic key recovery.