The Export of Cryptography in the 20th Century and the 21st*

Whitfield Diffie and Susan Landau
Sun Microsystems, Inc
Palo Alto CA

April 19, 2005

August 2000

On the 14$^{\text{th}}$ of January 2000, the Bureau of Export Administration issued long-awaited revisions to the rules on exporting cryptographic hardware and software. The new regulations, which grew out of a protracted tug of war between the computer industry and the U.S. Government, are seen by industry as a victory. Their appearance, which was attended by both excitement and relief, marked a substantial change in export policy. This paper examines the evolution of export control in the cryptographic area and considers its impact on the deployment of privacy-protecting technologies within the United States.

Before the electronic age, all "real-time" interaction between people had to take place in person. Privacy in such interactions could be taken for granted. No more than reasonable care was required to assure yourself that only the people you were addressing — people who had to be right there with you — could hear you. Telecommunications have changed this. The people with whom you interact no longer have to be in your immediate vicinity; they can be on the other side of the world, making what was once impossible spontaneous and inexpensive. Telecommunication, on the other hand, makes protecting yourself from eavesdropping more difficult. Some other security mechanism is required to replace looking around to see that

---

*To appear in the *Handbook of the History of Information Security* Elsevier B.V.

1

no one is close enough to overhear: that mechanism is cryptography, the only security mechanism that directly protects information passing out of the physical control of the sender and receiver.

At the turn of the 20th century, cryptography was a labor-intensive, error-prone process incapable of more than transforming a small amount of written material into an encoded *ciphertext* form. At the dawn of the 21st it can be done quickly, reliably, and inexpensively by computers at rates of a billion bits a second. This progress is commensurate with that of communications in general yet the fraction of the world's communications protected by cryptography today is still minuscule. In part this is due to the technical difficulty of integrating cryptography into communication systems so as to achieve security, in part to an associated marketing problem. Proper implementation of cryptosecurity requires substantial up-front expenditure on infrastructure while most of the benefit is lost unless there is nearly ubiquitous coverage, a combination that deters investment. These factors result in a lack of robustness of the market that makes it prey to a third factor, political opposition.

As telecommunication has improved in quality and gained in importance, police and intelligence organizations have made ever more extensive use of the possibilities for electronic eavesdropping. These same agencies now fear that the growth of cryptography in the commercial world will deprive them of sources of information on which they have come to rely. The result has been a struggle between the business community, which needs cryptography to protect electronic commerce and elements of government that fear the loss of their surveillance capabilities. Export control has emerged as an important battleground in this struggle.

Background

In the 1970s, after many years as the virtually exclusive property of the military, cryptography appeared in public with a dual thrust. First came the work of Horst Feistel and others at IBM that produced the U.S. Data Encryption Standard. DES, which was adopted in 1977 as Federal Information Processing Standard 46, was mandated for the protection of all government information legally requiring protection but not covered under the provisions for protecting classified information — a category later called "unclassified sensitive."

The second development was the work of several academics that was to lead to *public-key cryptography*, the technology underlying the security of

internet commerce today. Public-key cryptography makes it possible for two people, without having arranged a secret key in advance, to communicate securely over an insecure channel. Public-key cryptography also provides a digital signature mechanism remarkably similar in function to a written signature.[1] The effect of new developments in distinct areas of cryptography was to ignite a storm of interest in the field, leading to an explosion of papers, books, and conferences.

The government response was to try to acquire the same sort of "born classified" legal control over cryptography that the Department of Energy claimed[2] in the area of atomic energy. The effort was a dramatic failure. NSA hoped an American Council on Education committee set up to study the problem would recommend legal restraints on cryptographic research and publication. Instead, it proposed only that authors voluntary submit papers to NSA for its opinion on the possible national-security implications of their publication.[3]

It did not take the government long to realize that even if control of research and publication were beyond its grasp, control of deployment was not. Although laws directly regulating the use of cryptography in the U.S. appeared out of reach — and no serious effort was ever made to get Congress to adopt any — adroit use of export control proved remarkably effective in diminishing the use of cryptography, not only outside the United States but inside as well.

---

[1] In recognition of the increasing importance of electronic commerce, in June 2000, President Clinton signed into law the Millennium Digital Commerce Act, Public Law 106-229, which establishes the legal validity of "electronic signatures." The term is somewhat broader than "digital signature" but points the way toward a future in which alternatives to the written signature play a central role in commerce.

[2] The courts have never ruled on the constitutionality of this provision of the *Atomic Energy Act of 1946. U.S. Statutes at Large* 60 (1947); 755-75. In 1997, the Progressive magazine challenged it by proposing to publish an article by Robert Morland entitled "The H-bomb Secret, how we got it, why we're telling it." After the appearance of an independent and far less competent article on how h-bombs work, the government succeeded in having the case mooted and leaving the impression in the popular mind that it would have won. In fact, the virtual certainty that it would have lost is undoubtedly why it acted as it did.

[3] Susan Landau, *Primes, Codes and the National Security Agency,* 30 Notices of the American Mathematical Society 7, at 10 (1983).

Export Control

The export control laws in force today are rooted in the growth of the Cold War that followed World War II. In the immediate post-war years the U.S. accounted for a little more than half of the world's economy. Furthermore, the country was just coming off a war footing, with its machinery of production controls, rationing, censorship, and economic warfare. The U.S. thus had not only the economic power to make export control an effective element of foreign policy but the inclination and the regulatory machinery to do so.

The system that grew out of this environment had not one export control regime but two. Primary legal authority for regulating exports was given to the Department of State, with the objective of protecting national security. Although the goods to be regulated are described as *munitions*, the law does not limit itself to the common meaning of that word and includes many things that are neither explosive nor dangerous. The affected items are determined by the Department of State acting, through the *Munition Control Board*, on the advice of other elements of the executive branch, especially, in the case of cryptography, the National Security Agency.[4]

Exports that are deemed to have civilian as well as military uses are regulated by the Department of Commerce. Such items are termed *dual-use* and present a wholly different problem from "munitions." A broad range of goods — vehicles, aircraft, clothing, copying machines - - — are vital to military functioning just as they are to civilian. If the sale of such goods was routinely blocked merely because they might benefit the military of an unfriendly country, there would be little left of international trade. Control of the export of dual-use articles therefore balances considerations of military application with considerations of foreign availability — the existence of sources of supply prepared to fill any vacuum left by U.S. export bans.

The munitions controls are far more severe than the dual-use controls, requiring individually approved export licenses specifying the product and the actual customer as opposed to broad restrictions by product category and national destination. Legal authority to decide which regime is to be applied lies with the Department of State, which can authorize the transfer of jurisdiction to the Department of Commerce, a process called *commodities jurisdiction*.

Assessing whether a product is military or civilian is not always straight-

---

[4]U.S. Export control regulations are described at length in Root and Liebman's *United States Export Controls.*[Root]

forward. Once we leave the domain of the clearly military (such as fighter aircraft), we immediately encounter products that either have both military and civilian uses or products that can be converted from one to the other without difficulty. The Boeing 707, a civilian airplane, was a mainstay of the world's airlines during the 1960s and 1970s. Its military derivatives, the C-135 (cargo, including passengers), the KC-135 (tanker), and RC-135 (intelligence platform) have been mainstays of Western military aviation. Recognizing that civilian aircraft might be put to military use and thus bypass export control, the U.S. government nonetheless permitted their export as a business necessity. The allowability of exports was judged on the basis of how dual-use goods were configured and who was to be the customer. Generally speaking a commercial technology, not explicitly adapted to a uniquely military function, can be sold to a non-military customer without excessive paperwork.

The application of export controls naturally depends heavily on the destination for which goods are bound. Applications for export to U.S. allies, such as the countries of Western Europe, are more likely to be approved than applications for exports to neutral, let alone hostile, nations. Clearly the effectiveness of export controls will be vastly magnified by coordination of the export policies of allied nations. During the Cold War, the major vehicle for such cooperation among the U.S. and its allies was *COCOM*, the *Coordinating Committee on Multilateral Export Controls*, whose membership combined Australia, New Zealand, and Japan with the U.S. and most western European countries.[5] Although COCOM existed primarily to prevent militarily significant exports to non-COCOM countries, that did not mean that the COCOM countries exported freely among themselves. Many products that would not be permitted out of COCOM could be sold to other COCOM countries but still required a burdensome export approval process.

Export Status of Cryptography

In the post-WWII period, cryptography was, like nuclear energy, an almost entirely military technology.[6] It is stretching the point only a little to

---

[5]Iceland for some reason was not included.

[6]More precisely, the market for cryptography was almost entirely military. A small number of companies manufactured cryptographic equipment but found their best markets in governmental rather than commercial sales. These were the primary suppliers to nations that did not maintain a domestic capacity to produce cryptographic equipment. Even the United States — where most cryptographic equipment was produced by commercial firms

say that insecure analog voice scramblers or hand-authentication techniques that might be found in civilian uses were no more closely related to high-grade military encryption equipment than glowing watch dials or x-ray machines were related to atomic bombs. Not surprisingly, all cryptography, regardless of functioning or intended application was placed in the category of munitions. As the information revolution progressed — particularly as computers began to "talk" more and more to other computers — the argument for dual-use status slowly improved. Telecommunications between humans can be authenticated by combinations of more or less informal mechanisms: voice recognition, dial-back, request to know the last check written on an account, etc. To achieve high security in communication between computers without human intervention, cryptography is indispensable. Nonetheless, cryptography remained in the "munition" category long after this seemed reasonable to most observers.

The importance of the munition/dual-use distinction lies in a difference in licensing procedures and a difference in the criteria for export approval. As munitions, cryptographic devices required individually approved export licenses. Two factors combine to make such licenses antagonistic to commercial use of cryptography. One is time: the weeks or months required to get approval often exceed the time commercial organizations allocate to procurement of even major systems. The other is the requirement to identify the end customer. In much of commerce, manufacturers deal with one or more layers of resellers who may either be unaware of the identities of buyers or unwilling to share their information with their suppliers. Munitions are not only more cumbersome to export but more likely to be denied approval outright. The law regulating military exports makes no provision for the probable effectiveness of export policy. If an export is judged militarily imprudent, it is barred regardless of the likelihood that this action will actually prevent the would-be purchaser from obtaining equipment of the type desired.

Even after the business necessity and thus the dual-use character of cryptography had become clear, the problem of distinguishing military from civilian cryptosystems remained elusive. Some cases were straightforward. Systems specially adapted to work with military communication protocols — such as the MK XII IFF[7] devices that identify aircraft to military radars —

---

but under exclusive contract to the government — licensed its World War II field cipher system, the M-209, from the Swiss firm Hagelin Ag.[[]p. 427]Kahn

[7]Identification Friend or Foe

or those whose implementations were ruggedized for field use or satisfied arcane military specifications against radiation leakage could safely be classified as military. But what about cryptosystems running in ordinary commercial computing equipment in ordinary office environments? Such equipment performs very similarly whether in a general's office or in a banker's.

The challenge of export control is to develop a policy that interferes as little as possible with international trade while limiting the ability of other countries to develop military capabilities that threaten U.S. interests. This requires setting rules to distinguish military uses of technology from civilian ones. In the case of cryptography, the initial attempt was to classify cryptosystems as military or civilian by strength, much as guns might be classified by caliber. Small arms have civilian applications — from hunting and target shooting to personal protection and public safety — whereas artillery is purely military. The distinction, however, proved far harder to make in the case of cryptography than of firearms. A cryptographic system adequate to protect a billion-dollar electronic funds transfer is indistinguishable from one adequate to protect a top-secret message.

The Impact of Export Control on Cryptography

As the U.S. share of the world's economy has declined over the past five decades, export controls have become less effective as a mechanism of U.S. foreign policy. Worldwide growth of manufacturing capacity, particularly in military technology, has made many more products available from non-U.S. sources, while the associated growth of markets outside the U.S. has meant that the cost to U.S. businesses of export controls is far greater. In 1950, it cost U.S. companies little to be prevented from exporting something for which there were few foreign customers. Today, with a majority of potential customers outside the U.S., a product's exportability can make the difference between success and failure.

This change in impact of export controls has changed their role and export controls on cryptography have come to be used at least as much for their effect on the domestic market as the foreign one. Three factors have made this possible:

- The export market in computer hardware and software is huge. The typical American computer company makes more than half its sales abroad and must manufacture exportable products to be competitive.

- Security is always a *supporting feature*; no system exists for the primary purpose of being secure. To be usable and effective security must be integrated from scratch with the features it supports. Even when it is feasible, adding cryptography to a finished systems is undesirable.

- Making two versions of a product is complicated and expensive, particularly when, as is typically the case, domestic and foreign products must interoperate. Making a more secure product for domestic use, furthermore, points out to foreign customers that you have given them less than your best. These costs would be borne were the domestic demand for security great enough but so far it has not been.

The result of U.S. export controls has thus been to limit the availability of strong cryptography, not merely abroad but at home.

These policies, which put the interests of intelligence and law-enforcement agencies ahead of other national concerns, were made possible by the dominant, though far from invincible, position of U.S. companies in the world market for computer hardware and software. Security, though a small component of most computer systems, is often essential. By forbidding the export of systems with good security, the U.S. risks losing the business of security-conscious customers to foreign competition, thereby accelerating the development of the computer industries outside the U.S. The fast-growing computer industry in both Europe and Asia have been only too happy to challenge the U.S. position and, as the growth of the world wide web and electronic commerce made the commercial importance of cryptography more obvious, the U.S. government came under more and more pressure to amend its regulations.

<center>Events After the Cold War</center>

The end of the Cold War at the beginning of the 1990s set the stage for a change in export policy. The first move in industry's direction was a deal struck in 1992 between the National Security Agency, the Department of Commerce, and RSA Data Security, a leading maker of cryptographic software. It provided for streamlined export approval for products using approved algorithms with keys no longer than 40 bits.[8] Two algorithms, both trade secrets of RSA, were approved.

---

[8]If the encryption algorithm is properly designed, then the difficulty of unauthorized decryption is determined by the number of bits in the key; an increase of one bit doubles

The problem of keylength is not an issue that lends itself well to compromise and the strength represented by 40-bit keys could hardly have pleased either side. In 1992, a message encrypted using a 40-bit key could be cracked by a personal computer using the crudest techniques in a month or so — hardly sufficient for the lifetime of product plans, let alone personnel records. On the other hand, had such systems been applied to even a few percent of the world's communications they would have created a formidable barrier to signals intelligence. Intercept devices must determine in a fraction of a second whether a message is worth recording. Encryption, broadly applied, seriously interferes with this selection process. If a small enough fraction of messages are encrypted, then being encrypted marks a message as interesting and the message will be recorded. Too many encrypted messages, even weakly encrypted messages, will glut the interceptor's disks and frustrate the collection effort.

At approximately the same time, a case arose that was to demonstrate the difficulty of controlling not only cryptography but open-source software. Philip Zimmerman, a programmer without previous experience in the cryptographic world, wrote an email security program called "Pretty Good Privacy" or PGP that combined several of the most popular cryptographic techniques and employed keys far larger than permitted by export rules. A federal grand jury in San Jose investigated for over a year before dropping the case. The grand jury gave no explanation for its actions but an event on the other side of the country immediately suggests itself. MIT press, publishing arm of the Massachusetts Institute of Technology, published the source code of PGP. Even though the type was set in an OCR font for easy conversion to electronic from, the government made no attempt to challenge the implicit claim that a book, no matter how easily read by a computer, was protected by the First Amendment. [diffielandau]

Government attempts to control cryptography were not limited to its export strategy. In parallel with the keylength-based formula — which it presumably saw as an interim measure — the U.S. government tried to change the rules to give itself a permanent advantage. In early 1993, it moved to

the cost to the intruder. A good encryption algorithm with a 56-bit key is thus 2^{16} or 65,000 times more difficult to crack than one with a 40-bit key. It is often taken for granted that cryptosystems are as strong as their keys suggest and thus it is common to speak of 40-bit cryptography, meaning both that the keys are 40 bits long and that breaking the system takes approximately a trillion encryptions.

replace the fifteen-year-old, 56-bit, Data Encryption Standard with an 80-bit algorithm that provided a special *trap door* for government access.[9] Although the standard was adopted, it found few takers and was generally counted as a failure.

Looking back over the 1990s, it is hard to judge whether the Clipper program set the stage for the sequence of confrontations and compromises that followed or whether all were merely consequences of the same technological and market forces. The government made several attempts to establish the principle that it had the right to control cryptographic technology in order to guarantee its power to read intercepted messages.[10] Over the same period it restructured the export-control bureaucracy and relaxed the regulations.

While cryptography was classified as a munition, a would-be exporter was required either to seek an export license from "State" or request a transfer of jurisdiction to "Commerce." In 1996 the Department of Commerce Bureau of Export Administration was given direct authority over most cryptographic exports.[11] In the process, however, the personnel to carry out the new role were transferred from the State Department to the Commerce Department, creating a sense that there was likely to be more change of form than substance.

It is during the reorganization of the export-control machinery that Department of Justice personnel were first introduced into the process. In tune with this introduction, though somewhat ahead of it in time, was a move to shape the terms of debate by talking about signals intelligence in terms that were drawn more from law enforcement and less from the military. It was true then and is true now that most U.S. interception of communications is targeted not against criminals (no matter how loosely this term is used) but against other countries — largely countries we recognize and with many of which we are on friendly terms. Spying on your "friends" is and has always

---

[9]This was the infamous *Clipper* system, in which the keys were split and escrowed with Federal agencies.[United States Department of Commerce, National Institute of Standards and Technology, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard," *Federal Register*, 59, no. 27 (9 February 1994): ***, microfiche.]

[10]In a related move, the government scored a major victory. The Communications Assistance for Law Enforcement Act of 1994 gave it the power to require communications carriers to build wiretapping into their networks.

[11]This was done by adopting Department of State regulations authorizing shippers to go directly to the Department of Commerce for certain categories of goods, rather than submitting their applications first to the Department of State.

been an uncomfortable activity but much of the discomfort is mitigated by secrecy. A matter never spoken about creates few awkward pauses in conversation but to engage in a public debate one must have something to say. In the debate about encryption it was necessary for the government to say why it was seeking to expand its powers of interception. The answer was to point to an unholy trinity: terrorists, drug dealers, and pedophiles. Entirely lacking in popular support, these groups were in no position to step forth and speak out against being spied on.[12]

A rationale has its costs. Giving a law enforcement rationale made it hard to maintain the intelligence criteria and as the decade wore on, the government's proposals moved toward the needs of police — individualized court ordered surveillance, perhaps requiring the cooperation of a foreign judicial system — and away from the invisible broad spectrum surveillance that the intelligence community desired. The predictable consequence was that the intelligence agencies, realizing that their needs were not being met, became less vociferous in their support of crypto-control proposals.

In the summer of 1996 the National Research Council released its 18-month study on cryptography policy, *Cryptography's Role in Securing the Information Society,* (the *CRISIS* report) conceived at the time of the key-escrow proposal. Acting on a mandate from Congress, the NRC convened a panel of sixteen experts from government, industry, and science, thirteen of whom received security clearances. The panel was heavily weighted towards former members of the government — the chair, Kenneth Dam, for example, had been Under Secretary of State during the Reagan administration — and many opponents of the government's policies anticipated that the NRC report would support the Clinton administration's cryptography policy. It did not.

The report concluded that "on balance, the advantages of more widespread use of cryptography outweigh the disadvantages," and that current US policy was inadequate for the security requirements of an information society[13]. Observing that existing export policy hampered the domestic use of strong cryptosystems, the panel recommended loosening export controls and said

---

[12] Whether wiretapping actually plays a significant, let alone indispensable, role in combating any of these phenomena is hard to assess. See Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* at 189-191 and 233 (MIT Press, 1st ed 1998).

[13] Kenneth Dam and Herbert Lin, *Cryptography's Role in Securing the Information Society* at 300–301 (National Academy Press 1996)

that products containing DES "should be easily exportable"[14].

This was not a message the Clinton administration wanted to hear and no immediate effect on policy was discernible. In the fall of 1996 the government announced that a window of opportunity for export would run for the two years 1997 and 1998. During this window, manufacturers would be allowed to export Data Encryption Standard products quite freely if they had entered into memoranda of understanding with the government promising to develop systems with *key recovery*[15] during the open-window period. This approach did not even survive its own window. In September 1998, the rules were relaxed to permit freer export of products containing DES or other cryptosystems with keys no longer than 56-bits.

It was a classic example of "too little, too late." Users around the world had come to feel that cryptographic keys should be 128 bits long. Technical arguments to the effect that there was no point in making the cryptography stronger than the surrounding security system cut little ice with customers. Very strong cryptosystems seem to cost no more to build or run than weaker ones so why not have the strong ones.

The year 1996 also saw the start of Congressional interest in cryptography export. The absurdity of US export controls and the danger that they would have a devastating impact on the growing electronic economy led various members of Congress to introduce bills that would have diminished executive discretion in controlling cryptographic exports. None of the bills — which in their later forms were called SAFE for Security and Freedom through Encryption — was close to having enough votes to override a promised presidential veto. Nonetheless, Congressional support for the liberalization of cryptographic export policy was to grow over the next few years, a policy in keeping with previous Congressional decisions. A decade earlier, the Computer Security Act, contrary to the desires of the Reagan administration, placed civilian computer security research and standards under the control of the National Institute of Standards and Technology, rather than NSA.[16]

America's International Strategy

The end of the Cold War, realigned the world and made the "east ver-

---

[14]Dam and Lin *supra note 13* at 312

[15]The term "key escrow" had acquired a bad name.

[16]Diffie and Landau *supra note 12* at 68–69.

sus west" structure of COCOM inappropriate. The organization, which had existed since 1949, was replaced by a new coalition, the Wassenaar Arrangement, that included former enemies from the Soviet Union and the Warsaw Pact. The expanded organization, comprising 33 nations, is less unified than its predecessor and its procedures are less formal. Although member nations agree on a common control list, each country performs its own review. In behind-the-scenes negotiations in 1998 the Clinton administration scored a coup: Wassenaar agreed that "mass-market" cryptography using a key length not exceeding 64 bits would not be controlled.[17] The implication was that anything else would be but the Wassenaar Arrangement is subject to "national discretion," and various nations in the agreement had not previously restricted the export of cryptography. Would they now? The Clinton administration believed so. It looked as if export restrictions would stay. Then evidence surfaced suggesting that the U.S. might be using Cold-War intelligence agreements for commercial spying.

A U.S. signals intelligence network called *ECHELON* that had been in existence for at least twenty years came embarrassingly to light. The Echelon system is a a product of the UK-USA agreement, an intelligence association of the English speaking nations dominated by Britain and the United States. According to a report prepared for the European Parliament[18], Echelon targets major commercial communication channels, particularly satellite systems. Many in Europe drew the inference that the purpose of the system was commercial espionage, and indeed, former CIA Director James Woolsey acknowledged that was at least a partial purpose of the system.[19] Commercial communications play a large and growing role in government communications (both military and nonmilitary) and are thus a "legitimate" target of traditional national intelligence collection. It is the position of the U.S. that it does not provide covert intelligence information to U.S. companies.[20]

---

[17]The 64-bit limit was for symmetric, or secret-key, cryptography. This translates to approximately 650 bits for public-key cryptography. (Public key is typically used for key exchange; then the communication is encrypted via a secret-key algorithm using the key just negotiated.)

[18]European Parliament, Directorate General for Research, Directorate A, The STOA Programme, *Development of Surveillance Technology and Risk of Abuse of Economic Information.* Prepared by Duncan Campbell, April 1999, PE 168/184/ Part 4/4.

[19] James Woolsey, *Why We Spy on Our Allies,* Wall Street Journal, (17 March 2000, A18).

[20]The U.S. government says that it uses intelligence information to assist U.S. business in countering foreign corrupt practices.[21]

The potential targets of such spying could hardly be expected to regard U.S. policy as adequate protection under the circumstances. Consternation replaced cooperation in the European community. Nations whose policies had previously ranged from the no-controls stance of Denmark to the relatively strict internal controls of France, were now united on the need to protect their communications from the uninvited ear of U.S. intelligence and cryptography was key to any solution. European policies began to diverge from American ones.

The Rules Change

In 1999, a SAFE bill passed the five committees with jurisdiction and was headed to the floor of the House, when it was announced that the regulations would be revised to similar effect. The administration capitulated but avoided the loss of control that a change in the law would have produced.

On 16 September 1999, U.S. Vice President, and Presidential candidate, Albert Gore Jr.[22] announced that the government would capitulate. Beginning with regulations announced for December — and actually promulgated on 14 January 2000 — keylength would no longer be a major factor in determining the exportability of cryptographic products.

In its attempt to make a viable military/civilian distinction, the new regulations take several factors into consideration:

1. They define a concept of *retail* products, similar to the *Mass Market* products defined in the Wassenaar Arrangement.

2. They distinguish sharply between commercial and government customers.

3. They make special provision for software distributed in source code.

In the view of export control, an item is retail if it is:

- Sold widely,

- Sold in large volume,

- Made freely available,

---

[22]The Administration's anti-cryptography policy was inimical to Silicon Valley, whose support was seen as crucial for the Vice President's bid for President.

- Not customized for each individual user, and not extensively supported after sale.

- Not intended explicitly for communications infrastructure protection.

The definition is not entirely in accord with the everyday meaning of "retail" since many retail items are configured for each customer and some, such as custom tailored clothing, have no wholesale stage.

Retail items are largely free of control. They must be submitted for a "one-time review" that the government is supposed to complete within thirty days. If the would-be exporter has not heard anything within that time, it is free to ship its product. The government can demand additional information or even demand more time because the "review is not proceeding in an appropriate fashion"[23] but the rule is some improvement over the previous versions which required the exporting organization to wait until it received an export license from the government before shipping.

Items that are not retail are regulated primarily on the basis of the customer. For many items, commercial sales are acceptable but government sales are not. The distinction between government and the private sector is far from clear — what is the status of partly-government-owned PTT, for example? — and has been a continuing source of friction.

One especially interesting feature of the regulations is their application to software that may be distributed freely in source form but may not be used for commercial purposes without a license. In this case, the rules for distributing the software (by posting it on the Web, for example) are the same as for open-source software — it is only necessary to inform the Bureau of Industry and Security (formerly the Bureau of Export Administration) when you do it. Export approval is required prior to granting a license to a foreign customer, however.

The new rules go a long way toward achieving the objective enunciated earlier. They are a clever compromise between the needs of business and the needs of the intelligence community. Products employed by individual users, small groups or small companies are fairly freely exportable. Products intended for protecting large communications infrastructures — and it is

---

[23]Department of Commerce, Bureau of Export Administration, *Revisions to Encryption Items.* 15 CFR Parts 734, 740, 742, 770, 772, and 774, Docket No. RIN: 0694-AC11, Effective January 14, 2000. at § 4g

national communication systems that are the primary target of American communications intelligence — are explicitly exempted from retail status.

European Decontrol

In June 2000 the European Council of Ministers announced the end of cryptographic export controls within the European Union and its "close trading and security partners" which include the Czech Republic, Hungary, Japan, Poland, Switzerland, and the United States. The liberalized export regulations of January 14 would no longer provide the level playing field the U.S. Administration sought.

On July 17, 2000, in response to the European liberalizations, the Clinton administration adopted similar ones: export licenses would no longer be required for export of cryptographic products to the fifteen EU members and the same additional countries[24]. Furthermore, although companies would have to provide one-time technical reviews to the U.S. government prior to export, they would be able export products immediately.

Why Did it Happen?

What forces drove the U.S. Government from complete intransigence to virtually complete capitulation in under a decade? Most conspicuous is the Internet, which created a demand for cryptography that could not be ignored and at the same time made it more difficult than ever to control the movement of information but more subtle forces were also at play. One of these was the *open-source* movement.

Ever since software became a big business, most software companies have distributed object code and treated the source code as a trade secret. For many years, the open-source approach to software development — freely sharing the source code with the users — was limited to hobbyists, some researchers, and a small movement of true believers. In the mid-1990s, however, some businesses found that an open source operating system gave them more confidence and better reliability due to rapid bug fixes and the convenience of customization. Others discovered that they could make good money maintaining open-source software. The fact that sufficiently skillful and dedicated users could get free source code from the Web, compile it, configure it, install it, and maintain it did not mean that there were not other

---

[24]Australia, Canada, Czech Republic, Hungary, Japan, Norway, New Zealand, Poland, and Switzerland

users willing to pay for the same services.

Open source software has taken its place as a major element in the software marketplace. The consequence is a general decrease in the controllability of software. In particular, a serious threat to effectiveness of the government efforts to stop the export of software containing strong cryptography. A policy predicated on the concept of software as a finished, packaged product, one that was developed and controlled by an identifiably and accountable manufacturer foundered when confronted with programs produced by loose associations of programmers/users scattered around the world.

The problem is not merely one of enforcement. The government has always maintained that it could control the export of information but that view is hard to reconcile with the First Amendment and has never been thoroughly tested. A curious, but widely accepted, convention has grown up under which information of sufficiently limited circulation is not treated as having First Amendment protection. The maintenance manual for an aircraft may be a book but but it is treated more like a component of the aircraft than a publication. Proprietary source code was treated in the same way.

By comparison open source software was widely distributed — arguably published — on web sites. The Bureau of Export Administration might take the view that publishers of some programs required licenses but the legal basis of their position was doubtful and compliance was low. If a program, such as an operating system, leaves the U.S. without cryptography, foreign programmers can add cryptographic components immeasurably more easily than they could with a proprietary source operating system. U.S. export controls have little influence on this process.

To make that matter more arcane, the government has stopped short of claiming that source code published on paper lacks First Amendment protection, maintaining that only source code in electronic form is subject to export control.

In 1996, Daniel Bernstein, a graduate student at the University of California in Berkeley decided that rather than ignore the law, as most researchers had, he would assert a free-speech right to publish the code of a new cryptographic algorithm electronically. Bernstein did not apply for an export license, maintaining that export control was a constitutionally impermissible infringement of his First Amendment rights. Instead, he sought injunctive

relief from the federal courts. Bernstein won in both the district court[25] and the Appeals Court for the Ninth Circuit.[26] Unfortunately for the free-speech viewpoint the opinion of the appeals court was withdrawn in preparation for an *en banc* review — a review by a larger panel of Ninth-Circuit judges — that never took place. The appearance of new regulations provided the government with an opportunity to ask the court to declare the case moot. To the government's delight, the court obliged, indefinitely postponing what the government perceived as the danger that the Supreme Court would strike down export controls on cryptographic source code as an illegal prior restraint of speech.

A final adverse influence on export control came from the government's role as a major software customer and the military desire to stretch its budget by using more *commercial off-the-shelf* software and hardware. If export regulations discouraged the computer industry from producing products that met the government's security needs, the government would have to continue the expensive practice of producing custom products for its own use. This was uneconomical to the point of infeasible; the only way to induce the manufacturers to include sufficiently-strong encryption in domestic products was to loosen export controls.

The Aftermath of September 11th

On September 11th 2001, the United States was attacked by Al-Qaeda, a terrorist organization. There was no evidence to indicate that encryption played a role in the intelligence lapses that allowed the attack. Indeed, we now know that during the summer of 2001 intelligence garnered from terrorist communications prompted concern amongst the intelligence agencies that a major terrorist attack was imminent [[]pp. 235-6]Clarke [[]pp. 2-3]NC.

Nonetheless, a few weeks after the attacks, New Hampshire Senator Judd Gregg argued for controls on encryption. Neither the Bush administration nor other members of Congress joined Gregg, and, after several weeks, the Senator quietly dropped his efforts. The fact is that in combating terrorism, greater surveillance value appears to come more from traffic analysis than from wiretapping. For example, Osama bin Laden stopped using a cell

---

[25] *Daniel Bernstein v U.S. Department of State,* 922 F. Supp. 1426, 1428-30 (N.D. Cal. 1996)

[26] *Bernstein v U.S. Department of State* 176 F. 3d 1132, 1141, rehearing en banc granted, opinion withdrawn, 192 F. 3d 1308 (9th Cir. 1999)

phone in late 2001 because of tracking by U.S. intelligence in the mountains of Afghanistan. Meanwhile use of "anonymous" cellphones by al Qaeda members led to the arrest of a number of operatives and break-up of some cells [VanNatta]. U.S. intelligence agencies were well aware of terrorist threats before the events of September 11th. The government's shift in 2000 on cryptographic export controls occurred in this context and explains the the lack of support for Senator Gregg's proposal.

Conclusion

For fifty years the United States used export controls to prevent the widespread deployment of cryptography. This policy succeeded for forty of those years but changes in computing and communications in the last decade of the 20th century increased the the private-sector need for security and reduced the policy it to a Cold War relic. Its demise opens the way for securing the civilian communications infrastructure on which all of society will depend in the 21st century.

Recommendations

Although the new export regulations in the area of cryptography are a substantial improvement on earlier ones they still leave much to be desired.

- The regulations remain complex. The amendments, exclusive of surrounding procedural and explanatory material, amount to some dozen pages and the material they amend is several hundred.

- Although the burden of timeliness has on its face shifted from the exporter to the government, the conditions that permit the government to require more time are vague and appear to admit of discriminatory application. The use of these extensions should be precisely spelled out.

- The definition of retail is at some variance with the ordinary English use of that term. The regulations should perhaps return to the Wassenaar Arrangement's concept of "mass market."

- The notification requirements for open-source programs, although considerably less onerous than the earlier licensing requirements may still constitute an unconstitutional prior restraint on publication. Considering that they, like all of cryptographic export control, serve the interests

of the U.S. signals intelligence organizations, and that those organizations presumably watch the Web anyway, the notification requirements seem to serve little purpose.

- Although understandable from a U.S.-intelligence perspective, the restriction on infrastructure protection products may not be compatible with the U.S. desire to protect the critical infrastructure of the industrialized world from terrorist attack.

  This issue is fundamentally the same as those faced by the National Research Council CRISIS panel. We remind the readers of their conclusion, "On balance, the advantages of more widespread use of cryptography outweigh the disadvantages."[27]. We believe the same holds true for infrastructure protection. On balance, the advantages of more widespread use of cryptography for infrastructure protection products outweigh the disadvantages.

The shortcomings of export law in the cryptographic area are typical of the shortcomings of our export laws in general. Cryptography may therefore point the way toward a fairer export-control regime that balances the broad spectrum of United States interests rather than focusing on military security, which is not currently a major vulnerability. Such a regime, recognizing the importance of international commerce in the post-Cold War world would shift the much of the burden from exporters to the government. Foreign availability tests would be more broadly applied; exporters would be entitled to timely responses; a broader range of export decisions would be appealable to the federal courts; and the effectiveness of export policy would be subject to periodic review.

Bibliography

[AES] after 1http://csrc.nist.gov/encryption/aes/

[Bernstein96] after 1*Daniel Bernstein v U.S. Department of State*, 922 F. Supp. 1426, 1428-30 (N.D. Cal. 1996)

[Bernstein99] after 1*Bernstein v U.S. Department of State* 176 F. 3d 1132, 1141, rehearing en banc granted, opinion withdrawn, 192 F. 3d 1308 (9th Cir. 1999)

---

[27]Dam and Lin *supra note 13* at 6

[Campbell] after 1 Duncan Campbell, "Interception 2000: Development of Surveillance Technology and Risk of Abuse of Economic Information," Report to the Director General for Research of the European Parliament, Luxembourg, April 1999.

[Dam] after 1 Kenneth Dam and Herbert Lin, *Cryptography's Role in Securing the Information Society*, National Academy Press, 1996.

[Diffie] after 1 Whitfield Diffie and Susan Landau, *Privacy on the Line: the Politics of Wiretapping and Encryption*, MIT Press, 1998.

[Hager] after 1Nicky Hager, *Secret Power*, Craig Potton Publishing, New Zealand, 1996

[Kahn] after 1 David Kahn, *The Codebreakers*, Scribners, 1996.

[Landau83] after 1 Susan Landau, "Primes, Codes and the National Security Agency," *Notices of the American Mathematical Society*, [Special Article Series], Vol. 30, No. 1 (1983), pp. 7-10.

[NC] after 1 National Commission on Terrorist Attacks upon the United States, *Threats and Responses in 2001 (Staff Statement No. 10)*, April 13, 2004.

[Root] after 1 William A. Root and John R. Liebman, *United States Export Controls*, Fourth Edition, Aspen Law and Business Publications, 2002.

[USDoC1977] after 1 United States Department of Commerce, National Bureau of Standards (1977), "Data Encryption Standard," Federal Information Processing Standard Publication 46.

[USDoC1994] after 1 United States Department of Commerce, National Institute of Standards and Technology (1994), "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard," *Federal Register*, Vol. 59, No. 27, February 9, 1994.

[USDoC2000] after 1 Department of Commerce, Bureau of Export Administration: 15 CFR Parts 734, 740, 742, 770, 772, and 774, Docket No. RIN: 0694-AC11, Revisions to Encryption Items. Effective January 14, 2000.

[USHR 1999] after 1 U.S. House of Representatives, Select Committee on U.S. National Security, *Final Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the Peoples Republic of China*, 1999.

[VanNatta] after 1 Van Natta Jr., Don and Desmond Butler, "How Tiny Swiss Cellphone Chips Helped Track Global Terror Web," *New York Times,* 4 March 2004, p. A1.

[Woolsey] after 1 James R. Woolsey, "Why We Spy on Our Allies" The Wall Street Journal, March 17, 2000.