September 11th Did Not Change Cryptography Policy

Whitfield Diffie and Susan Landau

At the turn of the twentieth 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 turn of the twenty-first century, cryptography can be done quickly, reliably, and inexpensively by computers at rates approaching a billion bits a second. 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 expect 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 emerged as an important battleground in this struggle.

On January 14, 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, were seen by industry as a victory. These changes allowed the export of cryptography in retail products, without limit on the strength of the system. On September 11, 2001, the United States was attacked by Al-Qaeda, a terrorist organization. Although there was no evidence to indicate that encryption played a role in the intelligence lapses that allowed the terrible events of September 11th to occur, New Hampshire Senator Judd Gregg argued for controls on encryption. However, to the surprise of many who had not been following the encryption debate closely, Senator Gregg's call was not supported by the Bush administration or by other members of Congress, and, after several weeks of urging controls, the senator quietly dropped his efforts. In this communication we explain what caused the reversal of U.S. export policy on encryption and why the events of September 11th have not led to cryptographic controls.

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). Adopted in 1977 as Federal Information Processing Standard 46, DES 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.

The government response was to try to acquire the same sort of "born classified" legal control

Whitfield Diffie and Susan Landau are at Sun Microsystems, Inc. Susan Landau's e-mail address is susan.landau@sun.com. *Whitfield Diffie's e-mail address is* whitfield.diffie@sun.com. *Diffie and Landau are co-authors of* Privacy on the Line: The Politics of Wiretapping and Encryption, *MIT Press, 1998.*

over cryptography that the Department of Energy claimed in the area of atomic energy. The effort was a dramatic failure. The National Security Agency (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 [7, p. 10].

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 effective in diminishing the use of cryptography, not only outside the U.S. but inside as well. The export controls even had an impact on research [1].

Current export controls 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. The country was coming off a war footing, with its machinery of production controls, rationing, censorship, and economic warfare. The U.S. not only had the economic power to make export control an effective element of foreign policy but the inclination and the regulatory machinery to do so.

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. The affected items are determined by the Department of State acting—through the *Munitions Control Board*—on the advice of other elements of the executive branch. In the case of cryptography, this was primarily NSA.

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. Munitions controls are far more severe than the dual-use controls.

Application of export controls naturally depends heavily on the destination for which goods are bound. 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. The end of the Cold War realigned the world and made the "east versus west" structure of COCOM inappropriate. The organization was replaced by a new coalition, the Wassenaar Arrangement, that included former enemies from the Soviet Union and the Warsaw Pact.

In the post-WWII period, cryptography was an almost entirely military technology. 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. To achieve high security in communication between computers without human intervention, using cryptography to achieve authentication is indispensable. Nonetheless, cryptography remained in the "munition" category long after this seemed reasonable to most observers. As munitions, cryptographic devices required individually approved export licenses, which proved quite a burden for industry.

The problem of distinguishing military from civilian cryptosystems remained elusive. Some cases—such as the MK XII IFF[1] devices that identify aircraft to military radars—were straightforward, but many—such as cryptosystems running in ordinary commercial computing equipment in ordinary office environments—were not. 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. A cryptographic system adequate to protect a billion dollar electronic funds transfer is indistinguishable from one adequate to protect a top-secret message.

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. 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 on the foreign one. Three factors made this possible:

- The typical American computer company makes more than half its sales abroad and must manufacture exportable products to be competitive.

[1] *Identification Friend or Foe.*

- 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 system is undesirable.
- Making two versions of a product is complicated and expensive. Making a more secure product for domestic use, furthermore, points out to foreign customers that you have given them less than your best.

The result of U.S. export controls has 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 position of U.S. companies in the world market for computer hardware and software. But as the fast-growing computer industry in both Europe and Asia began to challenge the U.S. position, and 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.

The end of the Cold War at the beginning of the 1990s set the stage for a change in export policy. The first step, a deal struck in 1992 between the National Security Agency, the Department of Commerce, and RSA Data Security (a leading maker of cryptographic software), was not encouraging. It provided for streamlined export approval for products using approved algorithms with keys no longer than 40 bits.[2] 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, yet at the same time, any encryption applied to even a few percent of the world's communications would have created a formidable barrier to signals intelligence, which must determine in a fraction of a second whether a message is worth recording.

A few months into the Clinton administration, the government proposed *Clipper* as a compromise. Clipper was an exportable encryption system for "publicly switched telephones" in which the encryption keys would be *escrowed* with agencies of the federal government. The system, which was strongly opposed by industry and civil liberties groups, was eventually approved as a Federal Information Processing Standard, but never did well in the marketplace.

In response to the key-escrow concerns raised by Clipper, the National Research Council (NRC) released *Cryptography's Role in Securing the Information Society* (the *CRISIS* report) in the summer of 1996. 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, for an eighteen-month study. 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 U.S. policy was inadequate for the security requirements of an information society [4, pp. 300–1]. Observing that existing export policy hampered the domestic use of strong cryptosystems, the panel recommended loosening export controls and said that products containing DES "should be easily exportable" [4, p. 312]. This was not a message the Clinton administration wanted to hear, and no immediate effect on policy was discernible.

The year 1996 also saw the start of congressional interest in cryptography export. The absurdity of U.S. 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.

In behind-the-scenes negotiations in 1998 at the Wassenaar Arrangement the Clinton administration scored a coup: Wassenaar agreed that "mass market" cryptography using a key length not exceeding 64 bits would not be controlled.[3] The implication was that anything else would be. The Wassenaar Arrangement is subject to "national discretion," and various nations in the agreement had not previously restricted the export of cryptography. The Clinton administration believed that these nations would now begin to restrict cryptographic exports. 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

[2] *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 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.*

[3] *The 64-bit limit was for symmetric, or private-key, cryptography. This translates to approximately 650 bits for public-key cryptography.*

twenty years came embarrassingly to light. The Echelon system is 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 [3], 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 Central Intelligence Agency Director James Woolsey acknowledged that was at least part of the system's purpose [11]. 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.

In 1999, a SAFE bill passed the five House committees with jurisdiction and was headed to the floor, when the White House announced that the regulations would be revised to similar effect. By giving in, the administration avoided the loss of control that would have resulted from a change in the law.

On September 16, 1999, U.S. Vice President and presidential candidate Albert Gore Jr. announced that the government would capitulate.[4] Beginning with regulations announced for December—and actually promulgated on January 14, 2000—key length would no longer be a major factor in determining the exportability of cryptographic products.

The new rules split the market based on the type of buyer. *Retail* products could be freely exported. (An item is retail if it is sold widely in large volume, made freely available, not customized for each individual user, not extensively supported after sale, and not explicitly intended for communications infrastructure protection.) Windows NT with strong encryption would not be subject to export controls; custom-designed telephone switches would be. For nonretail items, export was freely permitted to commercial customers but restricted to government ones. Special provision was also made for software distributed in source code.

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

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

On July 17, 2000, in response to the European liberalizations, the U.S. 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. Furthermore, although companies would have to provide one-time technical reviews to the U.S. government prior to export, they would be able to export products immediately.

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 which at the same time made it more difficult than ever to control the movement of information. 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. That changed in the mid-1990s, as 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.

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 and, 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 identifiable and accountable manufacturer, foundered when confronted with programs produced by loose associations of programmers/users scattered around the world.

Open-source software was widely distributed—arguably published—on websites. If a program, such as an operating system, leaves the U.S. without cryptography, foreign programmers can add cryptographic components immeasurably more

[4] *The administration's anticryptography policy was inimical to Silicon Valley, whose support was seen as crucial for the vice president's bid for president.*

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 mathematics graduate student at the University of California, 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 [1] and the Appeals Court for the Ninth Circuit [2]. Unfortunately for the free speech viewpoint, the opinion of the appeals court was withdrawn in preparation for an *en banc* review by a larger panel of Ninth Circuit judges, a review 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's 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 being infeasible; the only way to induce the manufacturers to include sufficiently strong encryption in domestic products was to loosen export controls.

The decision in 2000 to change the export controls on cryptography was not made lightly. For fifty years the U.S. 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 twentieth century increased the private sector need for security and reduced the policy to a Cold War relic. Although the particular actions of September 11th were unanticipated, the fact that the changed export controls would lead to encrypted traffic being unreadable by U.S. intelligence was not. Nonetheless the National Security Agency signed off on the January and July 2000 liberalizations of cryptographic export controls. September 11th did not change the facts that led to the reversal of export control regulations governing cryptography, and it is not expected that controls will be reinstated.

References

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

[2] 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).

[3] 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.

[4] KENNETH DAM and HERBERT LIN, *Cryptography's Role in Securing the Information Society*, National Academy Press, 1996.

[5] WHITFIELD DIFFIE and SUSAN LANDAU, *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, 1998.

[6] DAVID KAHN, *The Codebreakers*, Scribners, 1996.

[7] SUSAN LANDAU, Primes, codes and the National Security Agency, *Notices of the Amer. Math. Soc.* [Special Article series], **30** (1983), 7–10.

[8] United States Department of Commerce, National Bureau of Standards (1977), Data Encryption Standard, *Federal Information Processing Standard Publication* 46.

[9] 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.

[10] 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 People's Republic of China*, 1999.

[11] JAMES R. WOOLSEY, Why we spy on our allies, *The Wall Street Journal*, March 17, 2000.