As the 20th century is drawing to a close, technology is now often shaping policy instead of policy shaping technology. Encoded electronic information is perhaps one of the more extreme examples of this phenomenon. Japan, which until very recently was considered an outsider, could potentially play the spoiler in U.S. and international cryptography policy formation and become an aggressive competitor in cryptographic products. Although currently Japan appears publicly uninterested in such a role, Japanese commercial interests in cryptographic technologies are growing as consumers utilize more on-line resources. The government ministries are also actively promoting cryptography research and development as part of an overall push to increase Japanese expertise in software. As the dominant engine of telecommunications and on-line development, the U.S. is the center of the most vociferous debates about cryptography and is pushing to mold an international consensus. But the U.S. debate has largely been devoid of any analysis of Japan’s potential role, thus leaving the U.S. open to being blind-sided by Japan.

Background and Technical Issues

There is an ever-changing mix of three competing and overlapping views regarding cryptography: those of business, government, and the individual. Ultimately, with varying degrees of emphasis, these three actors are found in all countries developing cryptographic technologies. Business is pushing technical development and wants to be able immediately to implement and capitalize on anything they develop and can market. Government, in the name of national security, wants to be able to listen in when necessary, similar to wiretapping telephones, but do their own encryption of sensitive information. Individuals want to keep government influence to a minimum and preserve their privacy. One measure of the strength of privacy concerns in the U.S. is that as of November 1997 there were over 40 privacy bills pending in the U.S. Congress.

Cryptography, the science of communicating in secret, is probably as old as writing. Indeed, writing itself, originally limited to an educated elite, was a form of secret communication. Modern cryptography begins in 1917 with the invention by Gilbert S. Vernam, of the American Telephone & Telegraph Company, of the Vernam System. This is well before the advent of powerful desktop computers, so encoding was done by special purpose machines. Famous examples from World War II include Enigma and Purple. The main problem with “old-style” cryptography is that the cipher, or the key to decoding, had
to be somehow passed to the receiving side. The whole operation could thus be easily compromised. In the case of Enigma, the code was actually broken by reverse engineering the code machine itself.

In May 1973, the U.S. National Bureau of Standards solicited proposals for an encryption system to be employed as a standard for all civilian sectors of the government. It was a watershed event in cryptography. The request stated that the successful proposal would have to be secure for at least five years in spite of the fact that the mechanism would be public and published. The resulting Data Encryption Standard (DES) was proposed by the IBM Corporation.

Simply put, the power of the cipher is based on complexity rather than secrecy. The basis of the DES is a pair of interlocking “keys” that must be utilized in tandem. One is known as the “private” key, the other as the “public” key. The private key is always kept secret by the original user. The public key is passed out to the whole world.

The combination of the two keys, makes possible the following: (1) When a user encrypts with the private key, people with the public key can decode it. That is probably a lot of people, but because only that pair of public and private keys work together, the person who decodes the message using the public key can be certain it came from a person with the private key. This is the basis of a “digital signature.” Only a person with the private key could have encrypted it. (2) Anyone with the public key can encrypt and send a message and only the user with the private key can read it. In sum, outgoing messages are certified, incoming messages are encrypted.

How then does an original user encrypt anything? How can two users communicate securely? For secure, verifiable communications in both directions, the other side will do the exact same thing: create a tandem of private and public keys, distribute the public key, and then be able to certify outgoing messages and decode incoming ones. In other words, as seen in the figure below, User X signs the message with his own private key and encrypts the message with the public key of User Y. Each message will then have a section certifying and a section encrypted, and the keys will have been passed back and forth publicly. There is no need to transfer the cipher to the other side in secret. There is a well-known analogy to describe public key encryption that uses the image of keys and lock-boxes. I create a key and lots of lock-boxes. I can send out these boxes everywhere and anyone can put something in one and lock it. But only I have the key to unlock the boxes. Analogous to wiretapping, the government would like to have a master key. “Key Escrow,” basically a huge library of everyone’s public and private keys, is the most talked about mechanism that would enable governments to listen in when necessary. In other words, individuals and businesses can encrypt their information, but they must give their private keys to the government so it can decode their messages. This is also known as a Public Key Infrastructure (PKI) or Certification Authority (CA). These systems would require an extremely high level of trust in government accountability. Particularly in the U.S., there is vigorous opposition to key escrow proposals. There are currently many different proposals for keeping key escrow separate from the government, including proposals to break up the escrowed keys into 3-5 different organizations, so that the
Modern encryption generally is based on a composite number of two primes multiplied together. The larger the prime numbers, the harder to decrypt. It is a distinct property of mathematics that factoring the composite number of two primes is much harder than multiplying them in the first place. Factoring is not impossible, however. Modern encryption is based on the idea that it is possible to make unauthorized decoding undesirable because too much time and resources would be required. The current export control of 56 bit keys is actually not strong and does not require much effort to decode. Therefore, 128-bit keys are now considered the standard, 1024-bit keys are exceptionally strong, and 4096-bit keys are essentially impossible to break.

The U.S. Data Encryption Standard (DES) of 56 bits, was originally issued in 1977 for protecting federal unclassified information. It was subsequently adopted as a voluntary industry standard (American National Standard X3.92-1981/R1987) and is widely used by the private sector. Under the provisions of the DES, the National Institute of Standards in Technologies (NIST) conducts a review every five years to determine whether the cryptographic algorithm specified by the standard should be continued, revised, or replaced. The first two reviews, in 1983 and 1988, resulted in the continuation of the standard. But the third review, which was completed in 1993, reaffirmed the DES for use only through 1998. It recognized that a new encryption standard might be needed by both government and industry after 1998.

There are other standards that are slowly beginning to be more widely adopted and that are stronger than the DES. A more secure method for using the DES algorithm in three operations, called Triple DES, has been developed by the private sector. On the government side, in January 1997, NIST announced that it would begin to develop an Advanced Encryption Standard (AES) that could replace the DES and that could be used by both government and industry. It is intended that this AES will specify an unclassified, publicly disclosed encryption algorithm available royalty-free worldwide, that is capable of protecting sensitive government information well into the next century.

Japan has been quietly making significant progress of its own in encryption development. In the summer of 1996, NTT Electronics Technologies Laboratory (now known as NTT Electronics, Inc.), a subsidiary of NTT, inadvertently shocked the American policy-making community by announcing it had developed a triple-DES chip that would break what were then (and still are) U.S. export controls. It was made clear that if foreigners could develop solid encryption technologies that become the standard, export controls by the U.S. government would merely cripple U.S. businesses’ ability to compete, while having no effect on national security. Criminals are just as happy to encode their plans using Japanese encryption software as American. The incident ended in something of a whimper as the Japanese government did its best to downplay the importance of its new technology, and so far no serious products have resulted from it. But clearly the Americans are not the only ones trying to replace DES. There are several other cutting-edge technologies, most of them in the early R&D stages in universities or industrial labs. Japanese researchers are
working on “Elliptic Curve Encryption,” which is a completely different mathematical algorithm, rather than one using just longer prime numbers.

The U.S. Policy Debate

In April 1993, the Clinton Administration made the first so-called Clipper Chip announcement—a proposal to include a special chip in each computer that would help decode information whenever the government deemed it to be necessary. Clearly, businesses were not happy with the idea of being forced to include extra hardware in their machines. Computers already in use would become obsolete, by law. It was a halting, poorly thought-out first step into cyberspace and was roundly criticized by all sides. In the face of such strong grass-roots opposition, the administration next proposed Clipper II and III, each trying to answer concerns raised by business and privacy proponents. The idea of a decoding chip was replaced with the idea of “key escrow,” where the government would keep a list of all private keys in escrow. The first proposals had the escrow placed in the Commerce Department. Since then, the government has proposed third-party escrow. The latest legislative initiative is SAFE (Security and Freedom through Encryption Act), which started in committee as a strong privacy-rights bill, but through amendments has been turned into an even stronger anti-privacy-rights bill.

Ultimately business is the catalyst for encryption debates. Business pushes development of new technology, utilizes the technologies first, and is extremely wary of government’s desire to regulate use. As a consequence of export controls, many companies must develop and market both domestic and international versions of their products that contain encryption software, with the version for the domestic market having a stronger level of encryption than the version for export to international markets. Along with the additional costs associated with the duplication of effort and expense in R&D, manufacturing, and distribution of different versions of products, companies face lost sales. Further, internally, U.S. firms with offices, vendors, and customers overseas desire the same level of security across their entire network. As Netscape has testified, “U.S. export restrictions on encryption impede American competitiveness in the high-wage information economy.”1 Meanwhile, the government has legitimate interests in being able to monitor criminal activities. Although they must be counter-balanced properly, the potential criminal use of highly-secretive, low-cost communications is a serious national security threat. In a letter to the New York Times (October 17, 1997), Louis Freeh, director of the FBI, stated unequivocally:

Encryption that cannot be deciphered regardless of the number of court orders or new technologies obtained by the police will devastate our ability to fight crime and prevent terrorism. It will nullify the ability to carry out court-authorized searches and seizures of criminal communication and electronic evidence... Policy decisions about encryption should not be left solely to market forces.
There is also the issue of protecting not only national security secrets, but industrial intelligence. The National Counterintelligence Center (NACIC), an arm of the U.S. intelligence community, concluded that “specialized technical operations (including computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses) account for the largest portion of economic and industrial information lost by U.S. corporations.”


In states that allow wire-tapping, an order for installation and use of a so-called “pen register,” which identifies the numbers dialed or transmitted on the phone line, or a trace device, used to identify the number from which a wire or electronic communication was transmitted, can be obtained if “the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation” (United States Code, Title 18). About how many wiretaps are conducted per annum? According to the FBI, in 1992, a total of 919 Title III orders, as well as an estimated 9,000 pen-register orders, were authorized for all federal, state and local law enforcement agencies. The FBI emphasizes that of that total, only 340 were procured by the federal government, of which only 252 were applied for by the FBI itself. According to other sources, in the years from 1982-1991, state and federal agencies conducted 7,467 taps, which have led to at least 19,259 convictions. The FBI claims that electronic surveillance is one of the most important investigative techniques used by law enforcement agencies. The reason such a critical tool has been used so sparingly, according to FBI Director Freeh, is that it is only employed in the most extreme cases, such as terrorism and drug trafficking. The U.S. government is therefore determined to install an escrow mechanism for Internet encryption, both domestically and internationally.

The rights of the individual, a constant political issue in the U.S., stretch back over two centuries before electronic cryptography existed. The known and suspected abuses of wiretapping (as well as other tools of law enforcement) provide fodder for supporters of a limited governmental presence in private lives. Electronic commerce provides an unparalleled opportunity for Big Brother to monitor individuals’ activities. Privacy rights groups want strong, unescrowed encryption technologies made available to individuals. This is perhaps most true in the U.S., but the sentiment is also found throughout Europe to varying degrees and even, minimally, in Japan.
International Issues

In the 1990’s, cryptography, along with the incredible popularity of the Internet and the visibility of many other on-line issues, has become mainstream in the U.S. By contrast, interest in foreign technology remains almost non-existent, although it does surface periodically. A New York Times editorial (October 3, 1997) entitled “An Attack on Privacy Rights” dated October 3, 1997, is scathingly critical of the most recent Congressional bill on this issue, SAFE: “The plan is unworkable because uncrackable encryption software is readily available abroad.” This view is largely in the minority, however, as most coverage tends to assume American technological hegemony.

Until 1996, when it was superseded by the Wassenaar Agreement, international import and export of encryption technologies were regulated by the Cold War era COCOM (Coordinating Committee for Multilateral Export Controls) agreement. Signatories of COCOM were: Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxemburg, Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, and the United States. Cooperating members included Austria, Finland, Hungary, Ireland, New Zealand, Poland, Singapore, Slovakia, South Korea, Sweden, Switzerland, and Taiwan. COCOM was an international mechanism for controlling the export of strategic products and technical data from member countries to proscribed destinations. In 1991, COCOM started allowing export of mass-market cryptographic software. Most member countries of COCOM followed its regulations, but the United States maintained separate, more stringent, regulations.

The main goal of the COCOM regulations was to prevent cryptography from being exported to “dangerous” countries. In practice, this usually meant the countries thought to maintain friendly ties with terrorist organizations, such as Libya, Iraq, Iran, and North Korea. Exporting to other countries not deemed dangerous was usually allowed, although states often required licensing.

COCOM was dissolved in March 1994 in anticipation of an improved agreement. Pending the signing of a new treaty, most members of COCOM agreed in principle to maintain the status quo, and cryptography remained on export control lists. In 1995, 28 countries established a successor to COCOM, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The negotiations on the treaty were finished in July 1996, and the agreement was ultimately signed by 33 countries. The Wassenaar signatories include all of the COCOM signatories and cooperating members except for Singapore and Taiwan, plus the following additional new members: Argentina, the Czech Republic, Romania, the Russian Federation, Bulgaria, and the Ukraine.

The Wassenaar Arrangement controls the export of weapons and of so-called “dual-use goods” that can be used both for military and civil purposes. Cryptography is an excellent example of a dual-use good. Generally, the provisions are similar to COCOM, although some restrictions have been refined and tightened. It is interesting that neither Singapore nor Taiwan, both major encryption developers and markets, have not signed the agreement. Currently, it also seems clear that Europe intends to resist U.S. policy designed
to create a system of international accords on key recovery for law enforcement. This development comes alongside the United States’ unexpected lurch towards heavy domestic and international encryption controls by Congress and the Federal Bureau of Investigation.

The Japanese Policy Debate

Where does Japan fit into this puzzle? Similar to other countries, there are three main players in the encryption debate in Japan: government, business, and private parties, but with government heading the list. The Japanese government molds and controls business activities to a much greater extent than in the U.S. and Europe, whereas Japanese privacy-rights concerns are still nascent at best. Part of this is attributable to a lack of knowledge— even more pronounced than in the U.S.—part is attributable to a lack of perceived need, due to less day-to-day use of electronic communications, and part is due to greater trust placed in the government by Japanese individuals.

The Japanese government was slow to understand the importance of encryption. Clear constitutional protection against electronic eavesdropping was perhaps the main reason that this lack of interest continued up through the early 1990’s. Article 21 of the constitution states that “Freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed. No censorship shall be maintained, nor shall the secrecy of any means of communication be violated” (emphasis added).

With the stunning increase of on-line use, this governmental attitude has quickly changed. Stewart Baker, former general counsel to the U.S. National Security Agency from 1992 to 1994, believes that, “there are strong signs that encryption is increasingly seen as a key technology for improving Japan’s penetration of the Global Information Infrastructure.” Although the Japanese government originally showed little interest in promoting encryption, it is significantly more concerned about catching up in this former defense technology now that its commercial possibilities are growing.

As a result of international agreements, Japan did restrict exports of encryption technology. As a member of COCOM, Japan maintained export controls on strategic arms, including encryption technology, for many years. Japanese companies were required to file documentation on the product and end-users of record, and the Ministry of International Trade and Industry (MITI) was supposed to investigate. After the 1987 “Toshiba Incident,” in which Toshiba was found to have exported machine tools to the Soviets that could be used in making submarines, MITI became stricter with export control investigation. Throughout the 1980’s, however, Japan did not have a commercial encryption industry, and therefore encryption exports were not a serious concern.

Recently, Japan has been promoting a more vigorous encryption industry. In late summer of 1996, the Clinton Administration, bowing to pressure from the U.S. high-tech industry, agreed to permit the export of 56-bit encryption products and comparable strength key exchange technology for legitimate uses in all but terrorist nations. Japan revised its key law regulating strategic exports (The Foreign Exchange and Foreign Trade Control Law) soon thereafter, and issued detailed regulations in September 1996, to be more in line with
trends in the U.S. In May 1997, MITI, no doubt looking to grab the administrative
guidance initiative, published a draft policy paper “Towards the Age of the Digital
Economy”. According to the draft, Japanese development of cryptography and
experimental projects should be promoted, and network users should be provided with
much more information about these technologies.

According to Baker, commercial interests have clearly become “predominant” in Japan,
with national security issues “hamstrung” by strong legal and constitution protections. This
is no doubt true, but it largely ignores the importance of MITI’s administrative guidance as
well as science and technology promotion budgets. Poor in software generally, and trailing
the U.S. in many telecommunications technologies, Japanese business has significant
ground to cover. The natural market will be in the U.S., which is likely to further hamper
Japan’s interest in going against U.S. policies. Even during Japan’s continuing poor
economic conditions, activity in the encryption field has been increasing, and more
products are expected.

MITI officials maintain that the Wassenaar Agreement requires end-user certification for
the export of high-security products, but that there are no restrictions on the export of any
software available to the public over the counter in Japan. This is similar to the U.S. and
most of Europe (minus France and Russia) where personal communication is still not
restricted, pending more debate. However, Stewart Baker believes that the Wassenaar
Agreement commits Japan to almost nothing, and leaves it in a position to challenge U.S.
companies’ dominance:

[Wassenaar] ...is unlikely to have much effect on Japanese
encryption exports. The agreement restricts sales to only a
handful of countries that are inconsequential as encryption
markets; it would not preclude Japan from selling encryption to
other countries. It calls only for notification of such sales-
notification that may occur after the fact.

He points out that in contrast, the U.S. places controls on exports to all major markets.
This is a potential problem where Japan is free to sell while the U.S. loses ground trying to
control encryption and create an international consensus. Current U.S. policy, Baker
argues, cannot survive for long against unrestricted Japanese competition for commercial
markets, should that ever occur. If Japan were to decide against international escrow
agreements and simply pushed strong unescrowed encryption, competitive forces would
“quickly doom any attempt to influence this technology through export controls and
standard-making.”

Japan is thus in a position to play the role of spoiler of any restrictive U.S. government
policy concerning encryption technologies. The U.S. government, meanwhile, is trying to
balance national security, business, as well as privacy concerns, but could potentially
hamstring U.S. business competitiveness. Japan has so far shown little interest in
undercutting the U.S., but in this area its espousal of unrestricted free trade-with the U.S.
in the unaccustomed role of trying to enforce restrictions—could create major trade problems down the road.

NOTES


JESSE S. CASMAN is director for research and information systems of the New Mexico US-Japan Center, where he supervises the web sites of JPRI, the Asian Technology Information Program (ATIP) of Tokyo, and the Japan Information Access Project of Washington DC. He is an advanced Japanese linguist, having studied at Middlebury, Doshisha, and the Interuniversity Center in Yokohama. His work with computers and the Internet has been widely recognized, including the University of Wisconsin’s recommendation of the JPRI site for social science researchers.