International Lawyer

Volume 31 | Number 3 Article 3

1997

Decoding OECD Guidlines for Cryptography Policy

Stewart A. Baker

ARTICLES

STEWART A. BAKER*

Decoding OECD Guidelines for Cryptography Policy

The Organization for Economic Cooperation and Development (OECD) Ad Hoc Group of Experts on Cryptography Policy Guidelines (under the auspices of the Information, Computers, and Communication Policy Committee) has completed a Recommendation concerning Guidelines for Cryptography Policy. The Recommendation sets out eight principles that should be followed by member nations in establishing their own cryptography policies. OECD recommendations are only that—recommendations—but because the OECD functions as a consensus forum for the most developed countries, the Guidelines are likely to have a significant international impact. This article analyzes the OECD's Recommendation in detail.

I. Background

Cryptography is a means of putting data in code. It allows people to transform a message or data into a form that can't be understood (decrypted) without knowledge of some secret information.

*Stewart A. Baker practices law at Steptoe & Johnson in Washington, D.C. His work in the private sector involves high-tech, mass media, and telecommunications issues, with an emphasis on international and appellate matters. Between mid-1992 and mid-1994, he was General Counsel of the U.S. National Security Agency, where he was involved in export controls and key-escrow encryption issues.

A user who wants to encrypt a message applies a mathematical function, called an algorithm, in order to scramble the message. The algorithm allows the user to select an individual "key." The algorithm then uses the key to encrypt the message. After the user sends the encrypted message, the recipient applies the same algorithm to decrypt the message. For a given algorithm, the strength of the cryptography increases with the length of the key, which is measured in bits.

An algorithm can be either a secret key algorithm or a "public key" algorithm. In a secret key algorithm, the same key is used for encrypting and decrypting. The advantage of a secret key algorithm is that it can provide very good security and does not take a lot of time to encrypt and decrypt data. The main disadvantage of a secret key algorithm is that it requires the sender and the receiver to decide on the key—and to share it securely—before they can send an encrypted message. This requirement is a problem because it precludes sending messages to complete strangers.

In a public key algorithm, the key used for encrypting is different from the key used for decrypting. Therefore, one of the keys can be made public. For example, one of the keys could be listed in a directory of users. This listing allows a complete stranger to send an encrypted message to anyone in the directory. The recipient can then use his or her private decryption key to read the message. The advantage of a public key algorithm is that correspondents who have never shared a single secret key in advance can exchange secure messages easily.

Three main reasons why a person might want to use cryptography are to ensure the confidentiality of data, to authenticate data, and to ensure the data's integrity. The OECD Guidelines use the term cryptography to refer generally to any of these functions. The term encryption is used to refer only to the use of cryptography to ensure confidentiality.

The use of cryptography for confidentiality (encryption) provides the ability to communicate privately. Individuals may not want a neighbor reading their mail, or may not want others to have access to their personal data. Businesses need to preserve the confidentiality of proprietary information, since safeguarding information (e.g., business plans or intellectual property) is vital to commercial success.

Cryptography can also authenticate a document (or some other piece of data). Cryptography allows the recipient of information to confirm that the information came from a certain sender (i.e., that the message is not a forgery). Authentication can prevent later repudiation: if the message is confirmed as authentic, the sender cannot easily deny that he or she sent the message. For example, digital signatures are a principal way to authenticate the identities of the parties in electronic commercial transactions, such as e-mail purchase orders or electronic funds transfers. Digital signing is usually done through a public key system. The sender encrypts the information with his or her private key, thereby signing the document, and sends the information to the recipient. The recipient decrypts the information

with the sender's public key, thereby verifying that the document indeed came from the sender.

Finally, using cryptography to ensure data integrity allows a person receiving a message to confirm that the message hasn't been altered in transit. This can be accomplished through the use of hash functions that are used to reduce the length of the information that must be encrypted and decrypted. Hash functions apply an algorithm to the information in order to produce a condensed message digest. The sender then encrypts the message digest using his or her private key and sends the original text and the encrypted message digest. The receiver then applies the same hashing algorithm to the original text to generate the same message digest, decrypts the sender's message digest using the public key, and compares the two message digests to determine if they are the same.

II. Government Regulation of Cryptography

Many governments are concerned about the widespread use of cryptography because of its potential to interfere with law enforcement investigations and intelligence gathering. Properly used, modern encryption offers an easy, cheap way to use present-day telecommunications with complete security. No criminal or terrorist organization has ever had this ability in the past, and governments, not surprisingly, are reluctant to embrace such a world with enthusiasm. At the same time, the ability to use global networks to share even the most sensitive data with trusted parties, the ability to guarantee the identity of complete strangers, and the assurance that messages have not been altered in transit hold out the prospect that the worlds of commerce and discourse may be forever transformed for the benefit of all. Not surprisingly, the many legitimate and beneficial uses of cryptography have led governments to search for ways to accommodate these competing interests.

One commonly proposed solution is the promotion of key-escrow or key recovery cryptography (also known as key escrow in the United States). This technology allows the person using cryptography to store a secret key with a trusted third party. The third party can return the key to the owner if the owner requires access to encrypted messages. A more likely reason to favor key recovery is the need of a surviving spouse to decrypt financial records, or the need of an employer to recover company files from an unhappy employee. Key recovery would also allow law enforcement or other governmental authorities to obtain access to decryption keys when authorized by law. Opponents of key recovery argue that criminals and terrorists would not deposit their keys with third parties, and that such systems would only introduce weaknesses into the process that could threaten privacy and security.

Some countries, such as France and China, restrict the domestic use of cryptography. In France, for example, a government authorization must be obtained in

order to use any cryptography for confidentiality purposes. As a practical matter, use of a cryptographic product in France is not likely to be authorized unless the cryptography is relatively weak (e.g., forty bit key lengths or less) or implements key recovery or trusted third party cryptography.

By contrast, the regulation of cryptography by the United States (as well as by several other governments) is done through export controls. In general, a license must be obtained in order to export cryptographic products and technical data from the United States. Certain license exceptions are available, however, for mass market cryptographic software that uses algorithms with a key length of forty bits or less and for products that have mandatory key recovery or similar features that allow for law enforcement access to the plaintext data.

While the most obvious (and the original) purpose of export controls on cryptography has been to discourage widespread foreign use of unbreakable encryption, another purpose of the U.S. controls is to encourage the development of an international key recovery infrastructure. By limiting exports to certain preferred types of cryptographic products, the U.S. Government hopes to make these products a standard, both inside and outside the United States. However, the U.S. Government realizes that these controls will ultimately be ineffective without the support and cooperation of other governments. For this and other reasons, the United States has sought to engage other governments on this issue and to encourage them to adopt consistent and complementary policies. One forum for this engagement has been the OECD.

III. The OECD

The OECD is an intergovernmental organization designed to foster multilateral discussions and co-operation on economic and social policies that have impacts beyond national borders. The OECD was formed in 1961 as a successor to the Organization for European Economic Cooperation, an organization formed after World War II to administer U.S. aid provided under the Marshall Plan to rebuild the war-ravaged economies of Europe. The OECD is now composed of twenty-nine countries, including many non-European members. OECD membership as of early 1997 includes: Austria, Australia, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, New Zealand, The Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

Much of the work of the OECD takes place in specialized committees and groups to which member countries send experts and policy makers. These committees and groups conduct research and issue recommendations and reports. This work is often made public in official OECD publications. Committees and groups for approximately 200 different subject areas currently exist within the OECD.

Although the OECD does publish formal guidelines and rules, these are not usually binding on member countries. The OECD does not have supranational legal powers—it merely provides a forum for voluntary cooperation among members. However, members often agree to at least take OECD guidelines into account in making policy, and OECD reports, publications, and guidelines can have a major impact on policy making in both member and nonmember countries.

IV. Background of the Cryptography Guidelines

The OECD Cryptography Guidelines are unusual in several respects. First, the process of drafting and adopting the Guidelines was marked by a remarkable sense of urgency, particularly for such an abstruse, yet politically charged, topic. The drafting took approximately a year from formal initiation to adoption, possibly a modern OECD record.

In addition, the Guidelines attracted an unprecedented degree of public attention. For all the usual diplomatic reasons—encouraging candor, flexibility, and frequent drafting experiments—OECD negotiations are traditionally conducted under a cloak of secrecy. In practice, because the negotiations often have implications for the private sector, there has been some discreet sharing of drafts and negotiating details between governments and their private sectors. But the cryptography talks produced such a high degree of attention from ordinary citizens and privacy advocates that what was once discreet sharing soon became routine publication of drafts in progress on the Internet. As disconcerting as the delegates and staff of the OECD found this attention, such attention is almost certainly a harbinger of all future OECD talks with implications for the private sector.

The initial impetus for the OECD talks came from the United States and was driven by the domestic American debate over cryptography export controls. Controls on cryptography exports were for many years a fairly noncontroversial feature of U.S. law. But the end of the Cold War, the rise of the Internet and other networks, and the growing availability of public key cryptography put new pressures on the old policies as the early 1990s wore on. United States computer software and hardware companies insisted that the ability to incorporate strong cryptography into their products would be the key to international competitiveness and that foreign companies unburdened by controls would take billions of dollars in sales from U.S. competitors. The U.S. Government responded that other countries were likely to have the same concerns as the FBI about criminal use of encryption, so that the end to U.S. export controls would simply mean the rise of import controls in other lands.

Partly to prove this prediction true and partly because it doubted its ability to maintain controls on cryptography without greater international support, the United States decided that the time had come to open multilateral talks on cryptography policy. Export controls on cryptography were the subject of discussion as part of what was then the CoCom, and is now the Wassenaar, Agreement. But

what the United States had in mind was something broader than export controls. The United States wanted to discuss domestic policy, law enforcement, and digital signatures, as well as national security and exports. With its focus on consensus, its prior work on computer security principles, and its concentration of high-tech economies, the OECD seemed the logical forum.

At the same time, other countries were also growing concerned about the issue. As the United States began allowing the export of increasingly strong cryptography, U.S. allies began to be concerned about the domestic law enforcement impact of cryptography. European Commission interest in the use of cryptography to facilitate European and global-networked commerce aroused concern that it would restrict the ability of European governments to control cryptography. France, which had domestic controls on cryptography, felt increasingly under siege. The United Kingdom, a traditional ally of the United States in cryptographic matters, was also concerned. Several countries, from Italy to The Netherlands, were also considering restrictions on cryptography, while many others—most notably Japan—viewed controls as unnecessarily restraining new technology. For all, the opportunity to influence U.S. and other nations' policies in this field had acquired new significance.

V. The Drafting Process

In any event, the U.S. initiative met with an enthusiastic response. After an informal meeting in December 1995, the work was taken up formally by the OECD in early 1996. There was also considerable support for the process in the private sector as well, in part because the U.S. Government made an early effort to involve its technology companies in the OECD process. First, every U.S. delegation included many representatives from the private sector, often more so than from the public sector, although the government never gave up its monopoly on the microphone. Second, and more important, the U.S. Government agreed that the OECD discussions would use as a starting point a discussion draft jointly prepared by the OECD's Business-Industry Advisory Council (BIAC) and the International Chamber of Commerce (ICC). The United States Council for International Business (USCIB), as the U.S. affiliate of the ICC and the U.S. liaison to the BIAC, was the principal author of the discussion draft.

The USCIB draft was enormously influential. Indeed, the basic structure of that draft, and its emphasis, remained more or less intact throughout the OECD process. As a participant in the USCIB drafting process, I would ordinarily be delighted to take some credit for this success, but the USCIB draft is also the source of some of the more vexing issues that lawyers and others face when trying to make sense of the Guidelines. Most importantly, it was the USCIB draft that first adopted the approach of simply listing competing principles to be implemented by governments, without giving governments much guidance about how to reconcile the obvious conflicts among the principles.

Drafting got underway in May 1996, and the USCIB draft was modified in a series of meetings and Secretariat drafts. The dynamic of the negotiation was established early. France, which already had domestic as well as export controls on cryptography, took the strongest position on the importance of regulation. The United States and the United Kingdom also took a view of cryptography that was shaped principally by the concerns of law enforcement and national security agencies. Canada, in contrast, was represented most vocally by a governmental privacy advocate whose views were most often in opposition to those of France, the United States and the United Kingdom.

Between these poles floated the remainder of the members. Several of these countries, most notably Japan, Sweden, and Germany, seemed to grow more sophisticated (and perhaps more sympathetic to the French-U.S.-UK view) as the talks wore on. Indeed, while it would be hard to say that the United States came away from the talks with a mandate for the cryptography policy it favored, U.S. policy makers were understandably pleased with the process as an educational device. By the talks' conclusion, more nations had cryptography policies, and these policies seemed more likely to take into account the concerns originally raised by the United States than was the case when the talks began.

VI. The Council Recommendation

The Guidelines are presented as an Annex to a Recommendation by the OECD's Council to its member countries. The Recommendation begins with a series of throat-clearing phrases, falling into four categories.

A. Having Regard to. . . .

Under the heading "Having regard to," the document lists a variety of related international instruments, including provisions of the OECD's organic documents, upon which the effort was founded; the previous OECD pronouncements on privacy, transborder data flows, and security of information systems; and a variety of multilateral agreements on export controls, privacy, and law enforcement.

B. Considering. . . .

Under this heading, the document sets out the very broad concerns that brought the cryptography project into being—the growth of global information networks, the commercial potential of these networks, and the importance of security in realizing that potential.

C. Recognising. . . .

Under this heading, the document lays out the specific contributions that cryptography can make to society. Cryptography may be used to provide confidential-

ity, authentication, anonymity, and integrity of data. It can protect the confidentiality of a wide range of critical data, and the failure to use cryptography can compromise a wide variety of interests, from privacy to national security. Apart from these unsurprising observations, this section also makes two more technical points. First, cryptography, no matter how good, cannot provide complete security; that depends as well on sound managerial and operational practices. Second, the use of cryptography to ensure integrity of data is quite distinct from the use of cryptography to guarantee the confidentiality of data. This second point—and its consequences for key recovery cryptographic systems—is discussed at more length in connection with the lawful access principle.

The remainder of this section makes the case for government policy making in the field of cryptography. After setting out the governmental responsibilities that may be affected by cryptography—from protecting privacy to enforcing the laws—the section notes that cryptography is not an unalloyed benefit. Cryptography may be used to conduct illegal activities of all kinds in secret, with serious consequences for society, so governments, along with industry and the public, must develop balanced policies. At the same time, the global nature of open networks, such as the Internet, makes incompatible national rules on cryptography imprudent.

Having said this, the document quickly clarifies that OECD recommendations of this sort do not trench on the sovereign rights of the OECD members to make whatever policies and to pass whatever laws they wish.

VII. Recommendations

The Recommendation next makes a series of particular recommendations to OECD member governments. It calls on them to establish or revise cryptography policies to reflect the Guidelines, and in that context renews two earlier recommendations that members adopt the OECD guidelines on information systems security and on privacy. The Recommendation calls on governments to disseminate the cryptography Guidelines to their citizens and, more importantly, to "consult, co-ordinate and co-operate" in implementing the Guidelines and to use the Guidelines as a basis for international agreements on specific cryptography policy issues. The Recommendation suggests that government remove or avoid creating unjustified obstacles to international trade in the name of cryptographic policy. The Recommendation urges governments to "state clearly and make publicly available" any national controls on cryptography and calls for an OECD review of the Guidelines at least every five years.

Many of the recommendations are unsurprising. Several are boilerplate phrases for the purpose of introducing the Guidelines. By referring to earlier guidelines on privacy and information systems security, the OECD was able to avoid repeating much language (and negotiation) already incorporated into those guidelines.

More interesting and significant was the inclusion of a specific recommendation that members avoid policies that create unjustified obstacles to trade and to the development of networks. This language is similar to injunctions contained in WTO agreements. By placing it on an equal footing with the recommendation that nations adopt the Guidelines, the OECD made avoidance of unjustified obstacles to trade an overarching recommendation that is both independent of the Guidelines and a lodestar for interpreting and applying all aspects of the Guidelines.

Also significant is the recommendation that governments make clear and public statements of their national cryptography policies. In fact, many nations have not stated their cryptography policies openly in the past. In the most egregious cases, business users have learned the scope of a nation's policy only when the authorities show up at their hotel or office seeking to confiscate unauthorized communications equipment. If followed faithfully, the OECD recommendation will move regulation of cryptography out of the shadows and into the normal world of business regulation.

VIII. The Guidelines

The meat of the Guidelines is in Section V, which sets forth eight principles to be applied by member countries in setting national cryptographic policy. Sections I and II cover the aims and scope of the Guidelines. Section III defines the terms used in the Guidelines; these definitions will be discussed when they appear in the principles themselves. Section IV makes an effort to reconcile the otherwise inconsistent principles set forth in Section V.

IX. Aims

This section sets out the intent of the Guidelines. One purpose is to promote the use of cryptography in order to foster confidence in networks and to help ensure data security and privacy on global networks. The second purpose qualifies the first: to promote the use of cryptography without unduly jeopardizing public safety and national security. Additional aims include raising awareness of the need for compatible cryptography policies and interoperable systems, assisting public and private decision makers in developing coherent policies and practices, promoting public-private cooperation in implementing those policies and practices, facilitating international trade through interoperable cryptography, and promoting international cooperation and standards for the use of cryptographic methods.

While none of these points are surprising, taken as a whole, the aims are notable for the insistent repetition of such themes as public and private sector cooperation, the need for international interoperability and standards, and internationally coordinated and compatible policies—all themes that are touched upon at least twice, in contrast to the single mention for law enforcement and national

security concerns. This imbalance, which seems to illuminate the OECD's intended weighing for purposes of setting cryptographic policy, shows up first in the Aims section but returns elsewhere in the document, most notably in the principles themselves.

X. Scope

In setting out the scope of the Guidelines, this section clarifies that they are aimed primarily at governments, though with an expectation that they will be widely read and followed in the private sector as well. The Guidelines do not apply to cryptography that protects military and diplomatic information, as such cryptography is ordinarily swathed in secrecy and cannot easily be subjected to Guidelines that call for international harmonization, open standard-making, and the like. Some nations nonetheless intend to apply the Guidelines even in protecting classified information. Although military and diplomatic cryptography is the best example of cryptography covered by this exception, the precise scope of the exception is difficult to measure. This difficulty is because different nations treat different kinds of information as classified or otherwise protected. The exception is therefore written broadly to cover data that "has been classified for national security or similar reasons" in order to allow for the wide variation in government classification schemes.

XI. Definitions

A central term in the Guidelines is cryptographic methods. This term incorporates a definition of cryptography that covers the use of any "cryptographic techniques, services, systems, products [or] key management systems." This definition in turn incorporates broad definitions of confidentiality, authentication, nonrepudiation, and integrity of data. In general, the principles speak of cryptographic methods when they mean the hardware or software that uses cryptography to provide encryption or other cryptographic tools such as digital signatures. It also broadly encompasses services that use cryptography to perform encryption, or other services related to digital signatures such as certification, and key management systems, including systems for depositing keys with trusted third parties or for otherwise distributing or maintaining keys.

XII. Integration

Taken individually, the eight principles of the Guidelines are often, though not always, unqualified statements that would be embraced warmly by some camps in the cryptography debate but only grudgingly by others. In other words, if the principles were treated as a menu from which governments could order at will, the Guidelines would provide little or no guidance to policy makers. This lack of guidance is because many of the principles, if applied alone, would

contradict or eviscerate others. For example, the privacy principle treats secrecy of communications as a fundamental right. A thoroughgoing application of this principle would render meaningless the principle relating to lawful access. Similarly, an aggressive application of the lawful access principle could dramatically restrict privacy.

The integration section tackles this difficulty head on, though not in a manner that lawyers will find entirely satisfactory. The document states that all eight principles are interdependent and should be implemented as a whole. It calls for a balance among the interests at stake, but it provides no further guidance to policy makers, who will understandably feel that the various principles often look in quite contradictory directions. In the end, then, the Guidelines and the integration section can best be seen as creating a series of policy objectives, all of which must be given some gravitational force. Perhaps one can best imagine the principles as fixed points, to which may be attached elastic bands of varying strengths. If all the bands are joined, the point at which they come to equilibrium will vary depending on the strength of each band. It is permissible under the Guidelines to attach strong bands to the lawful access principle and weak bands to the user choice principle, or vice versa. But to give no weight at all to any one of the principles is impermissible (with the possible exception of the lawful access principle, as we will see).

XIII. The Principles

A. Principle One: Trust in Cryptographic Methods

"Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems." This first principle is the foundation of the Guidelines, and is the logical starting point for analysis: Users of cryptography will only use products that they can trust.

While this principle may seem obvious, the history of cryptography is littered with examples of governments whose trust in their cryptography was misplaced. Cryptography is a complex and specialized area of expertise, and the field is full of competing commercial and national claims of superiority, combined with dark suggestions that competitive products are flawed in secret ways. Most consumers find these claims impossible to evaluate. The result is that choices of cryptographic method often resemble religious conversions more than comparison shopping. In times past, these difficulties have not been eased—indeed they have sometimes been exacerbated—by the acts of governments.

The evident purpose of this principle is to urge governments to start fostering rather than undermining trust in the advertised quality of cryptographic products. Among the suggested methods for encouraging trust is evaluation against criteria generated by the market. While governments themselves have often generated their own criteria for security systems in the past, the discussion under this heading is notably silent, and arguably disapproving, on this point.

The explanatory text also contains a somewhat lonely and peculiar statement to the effect that contracts dealing with the management of keys should state "the jurisdictions which apply." On its face, this statement seems to suggest that contracts for the management of keys should contain a clause on the law that applies—essentially a choice of law clause. Choice of law has some bearing on consumer trust, since different legal regimes may give the purchaser different rights. But when given such a reading, the sentence seems to be both too detailed and too tenuously tied to the trust principle to belong in the explanation of the principle.

A broader reading of the sentence would tie it more directly to the trust principle. Arguably, the sentence requires that contracts for the management of keys list all of the nations that have jurisdiction to demand lawful access to the keys. If so, it is a potentially sweeping rule aimed squarely at the private sector, and as such, a deviation from the OECD's traditional approach of making recommendations to governments.

Even if read simply as encouraging governments to adopt this rule in setting rules for the private sector, the rule is likely to prove unworkable. In many cases, determining which jurisdictions might be able to order production of cryptographic keys is a complex legal task. If a bank holds keys for its customers in its headquarters but has branches in fifty countries, how will the bank state the jurisdictions that apply? Does the bank list only the jurisdiction where its headquarters are located? Must the bank add the jurisdiction where the customer does his or her banking? Or must all fifty branch sites be listed? What about jurisdictions where the bank does business through subsidiaries? Any one of the jurisdictions might choose to assert a claim to records held by the bank. No one can definitely say how such a claim would be resolved, and it may be easier to include all possible jurisdictions than to make fine legal judgments about the scope of each jurisdiction's authority.

The prospect of such a burden will naturally lead companies to ask whether this statement actually imposes any obligation on them. An OECD document cannot create obligations on its own; this is particularly so with respect to stray statements in explanatory text rather than recommendations or principles. Even if the statement could be read as imposing an obligation on private actors, it applies to a limited, ill-defined class—persons or entities that have contracts dealing with the use of a key management system. Among other things, this class likely excludes corporate information technology personnel and offices that manage the keys of corporate employees, since they may manage the keys of employees but not pursuant to a key management contract. A more difficult issue is whether this class includes banks and other businesses whose business relationship with customers calls for much more than managing keys.

So what is covered by the phrase "contract dealing with the use of a key management system"? Given the other difficulties created by a broad interpreta-

tion of this statement, perhaps the wisest course is to assume that the phrase applies only to companies that explicitly and exclusively act as a key recovery agent—that is, to companies whose sole or principal business is the management of keys for purposes of lawful access. In the context of such a narrowly focused contract, it may be reasonable to expect that the customer will receive some information about which countries might be entitled to demand access to the customer's keys.

B. Principle Two: Choice of Cryptographic Methods

"Users should have a right to choose any cryptographic method, subject to applicable law." The first part of this principle is straightforward. Users need to be able to choose among cryptographic products or services in order to be able to trust the cryptography that they have chosen. The explanatory text includes a suggestion that those who own, control, access, use or store data may be responsible for protecting the data's confidentiality by employing cryptographic methods. This phrasing hints of legal duty and even legal liability for failure to use cryptographic methods in some circumstances. Precisely when such liability might arise is left unclear, but some European data protection legislation may impose an obligation to use cryptography at least on occasion. Any such obligation would naturally imply a concomitant right to choose adequate security measures.

The phrase "subject to applicable law" is more controversial. In general, the principle reflects agreement that users should be free to choose the cryptographic methods they want to use. At the same time, governments undeniably have the authority to limit user choice, either by export controls or by domestic controls on certain cryptographic methods. The reference to applicable law is evidently intended to recognize that many nations already have export controls limiting user choice, and at least one major OECD member, France, has domestic controls as well. To ensure that the reference to applicable law does not swallow the principle, the explanatory text includes two clarifications: (1) the phrase is not intended to encourage new regulation of cryptography, and (2) any government controls that are enacted should be no more restrictive than is essential to carry out the obligations of government and should respect user choice to the greatest extent possible.

Controls on cryptography exports or use are the most controversial forms of government regulation in this field. But the explanatory text also contemplates a second way in which governments may choose to regulate cryptographic methods: by enacting requirements that cryptography be used to protect certain kinds of data or that the public use cryptographic authentication, integrity, or nonrepudiation mechanisms in some circumstances. Such requirements should be imposed, the text suggests, only to protect an identified public interest, such as the protection of personal data or electronic commerce. One can only wonder what the point

of this limitation was thought to be. That such requirements would be imposed without serving some public interest is inconceivable, and requiring nations to identify that purpose publicly has less value in this context than in the context of Principle Eight, which uses somewhat similar language to better effect.

An interesting and difficult question left unanswered by the drafters is who is protected by this principle in an institutional context? Who are the users who have the right to choose? In most countries, an employer may insist on controlling all aspects of the information technology it provides to its employees. This would ordinarily include control of all cryptography used by its employees on the firm's network. Many companies are concerned about employees who depart without leaving behind the keys to encrypted company data. To ensure that they can always get access to company data, employers are likely to insist that employees use some form of key recovery mechanism.

But what if their employees are viewed as the users who have a right to choose any cryptographic method? Does this provision require that companies respect such a right, and what does that mean for a company's control of its network? Remarkably, this important question is not answered.

User is not defined, so an interpretation that turns corporate networks over to employees cannot be excluded out of hand, but the less likely reading. The principle is "subject to national law," and in most countries, the company's control over cryptography used on its network is assured by the applicable law. For this reason, the ambiguity would likely become meaningful only if a member nation were inspired by the provision to grant employees the right to choose cryptography independent of their employer's policy. While that sounds like a recipe for chaos, the text of the principle does not exclude such a result.

C. Principle Three: Market-Driven Development of Cryptographic Methods

"Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments." The phrasing of this principle is remarkably awkward. The principle's title suggests the intent of the principle is to urge that markets drive the development of cryptographic methods, yet markets are not mentioned in the principle. Where one might expect to find markets mentioned, one finds instead a bloviating reference to "the needs, demands and responsibilities of individuals, businesses and governments." Is this the same as the market? After all, to imagine who participates in markets other than governments, individuals, and businesses is difficult, and surely they participate in order to fulfill their needs, demands, and responsibilities.

So why the bloated circumlocution? Probably because the awkward phrase allows some governments to argue that markets alone should not call the tune, that markets must be constrained by governmental definitions of what is legitimate

in the private sector. The phrase also allows these governments to insist that the market must respond to the responsibilities and the demands of governments as well as private customers. Thus, like Principle Two, this principle is alloyed by words leaving governments free to intervene when they think unconstrained choice will not produce a socially responsible result.

When read in light of the explanatory text, however, the principle manages to overcome its awkward construction. The principle makes a fairly straightforward call for open and competitive market development of cryptographic methods. The principle as explained seems to be urging a departure from a long-standing government practice of developing and foisting on the private sector a variety of government-issue cryptography products. Thus, the explanatory text expresses a preference for bringing to the development of cryptography the rapidity and flexibility that characterize competitive technology markets. It also foreshadows Principle Four by calling for market-driven technical standards, criteria, and protocols in the field of cryptography.

D. Principle Four: Standards for Cryptographic Methods

"Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level." This principle lays heavy stress on the importance of standards in the development of cryptographic methods. It calls for the development of national and international standards, criteria, and protocols. In the explanatory text, this point is elaborated by asking that standards-making bodies work together with governments, business, and other experts to establish cryptographic standards, criteria, and protocols that respond to the needs of the market.

The text goes on to offer advice on the development of standards. The text notes at the outset that standards are to be developed "in response to the needs of the market." Nations are further cautioned that national standards should be consistent with international standards, because this consistency will facilitate global interoperability. Once standards, criteria, and protocols have been agreed upon, products and services must be evaluated against those standards and criteria if interoperability is to live up to its promise. The text also urges that if testing is performed against criteria or standards, then a strong effort should be undertaken to make sure that test results are broadly accepted.

The ultimate goals for the standards process are interoperability, portability, and mobility. In essence, interoperability means the ability of different cryptographic methods to work with each other effectively. Portability means the ability of cryptographic methods to be adapted and to function in any system—e.g., to move from one platform or operating system to another. Mobility means the ability of a cryptographic product to function in multiple countries or infrastructures.

E. Principle Five: Protection of Privacy and Personal Data

"The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptographic policies and in the implementation and use of cryptographic methods." While this principle seems on first reading to be fairly anodyne, it hides a wide gulf between what Americans call a right to privacy and what Europeans mean by the same phrase. Americans, weaned on the Bill of Rights, see the right of privacy as mainly protecting against governmental intrusions into the lives of citizens. For Europeans, protection of privacy usually means government regulations to protect individuals against corporate intrusions into their privacy and against corporate use of their personal data for commercial purposes.

That disparity produced a long and rather divisive fight in the 1970s over the OECD privacy guidelines. Businesses, especially those in the United States, feared the OECD was endorsing the imposition of a new European regulatory mandate on their activities. Principle Five of the cryptography Guidelines arguably adds to the body of the OECD work on privacy. First, the principle defines privacy as including secrecy of communications, as well as the protection of personal data. Secrecy of communications was not part of the definition of privacy in the 1980 guidelines.

Additionally, privacy is the only right identified in the principles as fundamental. That identification is understandable in the context of communications secrecy, which is the root concern that gave rise to the science of cryptography. That protection of personal data should be treated as fundamental to cryptographic policy making is less clear, particularly because this principle, as drafted, protects only the rights of individuals. The secrecy of corporate communications and the protection of confidential business information are not treated as fundamental, indeed are not even protected, by this principle.

The principle is a bit ambiguous on the question of who is supposed to be respecting the fundamental right of privacy. Is this principle designed to encourage the imposition of new obligations on private enterprises using cryptography? In general, the Guidelines are addressed to governments, and only governments make national cryptographic policies, so the principle is clearly aimed at governments when it urges that such policies respect the right to privacy. But the Guidelines can also serve as spurs to government regulation of the private sector. The principle urges respect for privacy in "the implementation and use of cryptographic methods," and many private enterprises implement and use cryptographic methods. Thus it would be logical to conclude that these Guidelines instruct private enterprises to respect individuals' privacy rights, including communications secrecy and personal data. Like the ambiguity in Principle Two about whether users are employees or employers, the language of this principle could, at a minimum, give comfort to governments that wish to impose new, privacy-related regulations on firms using cryptography.

The explanatory text continues this theme. The text begins with a nod toward

cryptography's contribution to privacy, including a favorable reference to its use in anonymous payment schemes. The text then devotes an equal amount of time to the theme of cryptography as a threat to privacy—certainly not the most intuitive approach to cryptography, but one that no doubt reflects the dominance of European-style privacy agencies in the OECD's discussion of this issue. Thus, the text voices concern over the privacy implications of cryptographic methods used to ensure data integrity in electronic transactions and that could allow personal identification or collection of personal data, but surely this is blindingly obvious. Indeed, the whole point of many digital signature schemes is to allow for personal identification and collection of personal data; one does not ordinarily expect to sign documents anonymously (although cryptography now makes that possible). While any signature or other identification of one's self has privacy implications, nothing is inherently intrusive about the use of cryptography for this purpose.

Fortunately, having expressed concern in passing about the privacy implications of some cryptographic methods, the OECD recommends no particular action, or at least nothing beyond its earlier recommendations on the protection of personal data. The implications of cryptography used for data integrity should be considered and explained, the document states, and when appropriate, privacy safeguards should be established. While this might seem to create a peculiar new obligation that falls more heavily on cryptographic identification systems than noncryptographic ones, the next paragraph clarifies the obligation to consider and to take action on any privacy implications.

This paragraph states that the OECD's earlier guidelines on privacy and personal data "should be applied in concert with national law when implementing cryptographic methods." In short, adherence to obligations assumed under the earlier guidelines is likely sufficient to fulfill the privacy obligations created by this principle. Since any other reading would create an imbalance between cryptographic and noncryptographic systems with the same privacy impact, this interpretation is the most plausible.

F. Principle Six: Lawful Access

"National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in these guidelines to the greatest extent possible." This principle was the centerpiece of the OECD talks. The principal reason the United States asked for a cryptography experts' group was to highlight the threat unrestricted cryptography poses to law enforcement agencies and to their ability to gain access to evidence of crimes. Without some recognition that the need for lawful access is a major factor in cryptography policy, the United States, France, and the United Kingdom would not have had much reason to endorse the Guidelines. The proposal remains controversial, however, especially among countries not planning to encourage key-recovery systems at home. The principle is therefore limited in many significant respects.

For example, this is the only principle that does not make a recommendation to governments. This principle does not say that members should adopt lawful access regimes, only that they may do so.

Similarly, no other principle is qualified by an entire sentence intended to restrict its scope: the lawful access policies of governments, the principle declares, "must respect the other principles to the greatest extent possible." This is also the only place in the principles themselves when the verb "must" is used, a remarkable deviation from the normal OECD practice of never issuing mandates to its member nations. The most reasonable reading of this second sentence is that it deliberately subordinates the lawful access principle to the other seven principles. On that reading, the sentence supplements the integration section, which otherwise calls on governments to respect all of the principles in implementing lawful access proposals. Such a reading is also consistent with the explanatory text of Principle Two, which pointedly states that any regulation of cryptography should respect user choice to the greatest extent possible. The explanatory text for this principle elaborates on the same theme. It notes—in a particularly tortured passage—that key management systems (presumably key recovery systems that allow for access) "could provide a basis for possible solutions which could balance the interests of users and law enforcement authorities." This passage is hardly a resounding endorsement of systems that provide lawful access. To drive that point home, the explanatory text declares that the OECD's adoption of the lawful access principle "should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access."

1. *Lawful Access*

What is lawful access? The idea has roots in the U.S. Government's "Clipper" chip, which combined strong encryption with a mechanism for storing the encryption keys with two separate escrow agents who would turn the keys over to the police if presented with a wiretap order or search warrant. The idea was to guarantee absolutely secure communications to law-abiding users without doing the same for law-breakers. While the idea has evolved in U.S. policy-making circles, the essential elements remain the same: storage of encryption keys with someone independent of the person using the encryption so that the police can gain access to encrypted communications under process of law.

This basic concept is reflected in the Guideline's definition of lawful access: "access by third-party individuals or entities, including government entities, to the plaintext, or cryptographic keys, of encrypted data, in accordance with law." This definition refines the original Clipper concept in several respects. First, it allows access by third-party individuals or entities, not simply by police or governmental authorities. Other than the police, who would seek access? Who are these third parties? Actually, before one can ask who the third parties are, one must guess at who the first and second parties are; these terms are not defined or used. Presumably the first party is the original user of the encryption and the

second party is the authorized key holder or key recovery agent. As for third parties other than the police, the usual examples are a business seeking to decrypt business files left behind by an employee who has died or decamped, or the heirs of an investor whose financial records were encrypted before death.

The text also speaks of access "to the plaintext, or cryptographic keys, of encrypted data." The concept of lawful access is defined broadly to include access to plaintext rather than simply access to keys because the drafters could not predict how key or data recovery services might evolve. The chosen language therefore allows for the creation of keyholding entities that always keep keys secret and that simply provide decryption services when access is required by the police or by other parties.

2. *In Accordance with Law*

The definition does not explain what is meant by access "in accordance with law." The processes for police search or wiretap warrants are fairly well-developed in most member countries. But how do third parties other than the police obtain access in accordance with law? Presumably subpoenas and similar civil orders will suffice to establish the right to access, but what about parties who have never needed to get court orders before? Employers who wish to recover data from computers used by their workers do not usually get court orders; they rely on their broad legal right to establish conditions of employment and to control data generated on their time and equipment.

The explanatory text, unfortunately, offers only modest comfort to employers in those circumstances. The text says that anyone requesting access to keys "must have a legal right to possession of the plaintext"—something an employer no doubt has—but must also request it "under legal process." This process is arguably different from judicial process, but certainly suggests that employers or others could be required to observe new formalities when they seek to recover encrypted data—even though they could have recovered the plaintext without formalities if the data had never been encrypted.

Whatever the passage means, it is clearly important to many OECD members. The passage is one of the few uses of the word "must" in the explanatory text. Almost all of the other uses occur in the explanatory text of this principle, where "must" is used to reinforce limitations on lawful access. The drafters evidently felt so strongly about the need to restrict the lawful access principle that they were willing to walk again and again to the edge of giving a direct order to member governments.

The explanatory text sheds further light on what the OECD considers to be an appropriate set of rules for granting lawful access. The document calls for a system that records instances of lawful access so that such disclosures can be audited for conformity with national law. The text urges that the fruits of access "must only be used for lawful purposes"—another use of "must"—and declares that any access should be subject to "time limits appropriate to the circum-

stances." In addition, the Guidelines recommend the rules for lawful access be stated clearly in a publication readily available to all concerned parties.

3. *Access to Signature Keys*

The explanatory text also tackles the emotionally charged question of third-party access to private authentication keys—as distinct from encryption keys. Access to authentication or signature keys is problematic because it would allow the possessor of the signature key to impersonate the proper owner of the signature. For this reason, the explanatory text uses the strongest possible language to insist that lawful access procedures "must recognize the distinction between keys which are used to protect confidentiality and keys which are used for other purposes only." The consequences of the distinction are spelled out starkly: cryptographic keys that are used only to provide for identity or integrity "should not be made available" under lawful access regimes without the consent of the owner of the key.

For most countries this injunction will cause little difficulty. All OECD governments agree they have little or no legitimate need to obtain private authentication keys or to impersonate individuals or companies. They also agree that the risks of permitting access to authentication keys are potentially enormous. For this reason, most countries that have considered the issue have adopted blanket policies against seeking access to private authentication keys.

Unfortunately, not all nations can provide such a blanket assurance. Some Asian countries, like Japan, have a long tradition of signing documents with a special seal or stamping device, known in Japan as a "hang-ko." These identification devices are purchased specially by individuals, registered with the authorities, and used in preference to handwritten signatures for formal, important transactions such as land sales. If the transaction is later challenged, the validity of the signature is determined by bringing each party's hang-ko to court, repeating the sealing process, and comparing the two seals. If this tradition were carried unchanged into the digital age, it might be necessary to reproduce the digital signing process in order to show the validity of the original signature, and this could require access to the private key. As a practical matter, however, such access will almost always be obtained with the consent of the party trying to prove the validity of his or her signature or will be obtained under the same protections offered today to hang-ko, which already must be protected against the risk of misappropriation and impersonation. Therefore, while the language of the explanatory text is quite sweeping in excluding government access to signature keys, that Asian courts will have any difficulty accommodating both new signature technology and the spirit of the OECD Guidelines is unlikely.

4. *Providing v. Verifying Identity*

While the intent of this explanatory paragraph is clear enough, the words are not. Some confusion is likely to arise in trying to interpret the scope of the

restriction. The text tells governments that they should not seek access to a "cryptographic key that provides for identity or integrity only" (as distinct from a cryptographic key that verifies identity or integrity). This is particularly confusing because the preceding sentence draws a careful distinction between keys used for confidentiality and keys used for other purposes only. Yet in this sentence, confidentiality keys are not even mentioned. Instead, we are asked to distinguish between keys that provide for identity and those that verify identity and are told that governments may have access to the second but not to the first. What gives?

The answer can be found in the intricacies of public key cryptography. In most such systems, there are two matched keys. One is a published, widely available key that can be used by anyone to encrypt messages; for mathematical reasons these messages can only be decrypted by the holder of the private or secret key. Such systems can also be inverted to prove identity: a message can be signed by the holder of the secret key. This message can only be verified by use of the published key. While anyone can verify such a message, only one person could have sent it—the holder of the secret key. Or so the theory goes. In practice, the validity of that conclusion depends on faith that the sender really managed to keep his secret key secret; government access to the secret key would destroy that faith. But of course the government, like anybody else, must have access to the public key in order to verify the identity of the message-sender.

With that detour, let's try to unpack the peculiar language of this paragraph. First, the language insists on a distinction between keys used for confidentiality and keys used "for other purposes only." This distinction is essential because it is possible to use exactly the same keys to encrypt secret messages and to sign documents. That is how mathematicians originally thought public key systems would be implemented, but in the real world people often want to compromise secrecy without losing identity (I'd like my secretary to be able to read my e-mail without also being able to sign my checks). When public key cryptography is implemented in accordance with the mathematicians' original vision, governments gaining access to the secret key used to decrypt messages must necessarily gain access to the secret key used to sign messages. The Guidelines do not attempt to prevent such access. Only when the signing key cannot be used for confidentiality is it considered sacrosanct.

What about the second sentence, with its distinction between keys providing for identity and those verifying it? The answer is that two keys are needed for digital signatures. The secret key used to sign a document is apparently the key that provides for identity in the OECD's lexicon, while the public key is the key that verifies identity. Since governments, like others, must have access to the public key for digital signatures to be meaningful, the Guidelines are careful to prohibit access only to the secret key used to provide for identity. This is neither the most intuitive phrasing nor the most careful drafting to be found in the Guidelines, but after detailed study the passage does eventually yield a coherent result.

G. Principle Seven: Liability

"Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated." Liability concerns have proven to be a large factor in the development of cryptography systems, including systems that facilitate lawful access. Fear of liability can push companies toward using cryptography to protect professional confidences or personal data. This fear can push companies toward the use of particular cryptography standards; the popularity of the United States' Digital Encryption Standard (DES) with banks may be due in part to the notion that banks cannot plausibly be sued for security flaws that may be discovered in a system endorsed and used by the U.S. Government itself. Fear of liability may also affect key recovery systems. Some users of cryptography are concerned they will be held liable if the failure to use key recovery means that they cannot recover encrypted data for a customer or for a government agent. At the same time, fear of liability has discouraged most large companies from entering the business of being a key recovery agent. Finally, opponents of key recovery have argued that governments must be liable for misuse of keys that they obtain through lawful access procedures.

1. *Contract v. Legislation*

This principle, which was suggested in the original draft prepared by business groups, provides general guidance for all of these issues. The principle begins by noting that liability may be established by contract or by legislation. Strikingly for a document endorsed by a forum of governments, legislation is listed after contract as a method of establishing liability.

This listing is surely not an accident. The explanatory text makes it even more plain: in the first instance, liability "should be made clear by contract," which may be supplemented "where appropriate" by legislation or international agreement. This principle favors contractual assignments of liability over governmental regulation in part as a way to give full effect to the other principles, particularly those favoring the widest possible user choice and market-driven product development. Imposition of a single set of liability rules on users and developers of cryptographic systems tends to reduce choice and the role of the market in sorting out liability.

2. *Market Scenarios on Liability*

For an example of how liability might be established by contract, imagine two plausible uses of key recovery mechanisms. In one arrangement, Quick Corp. enters into a contract with Keyholders, Inc., to manage Quick Corp.'s encryption keys. Quick Corp. is most concerned about getting its keys back quickly on weekends or holidays with little or no delay. It may want Keyholders, Inc., to

provide access to encryption keys by telephone to any Quick Corp. employee who knows a special pass phrase. This is a quick system, but the system is not secure. Keyholders, Inc., might agree to such an arrangement, and it might be willing to charge a fairly low fee for each key released, but only if it could limit its liability to, say, $1,000 in the event that some outsider learns the pass phrase and tricks Keyholders' staff into providing a key improperly.

Now imagine an equally plausible but quite different scenario. Because of the sensitivity of certain of its encrypted data, Sure Corp. wants Keyholders, Inc., to release keys only if the CEO of Sure Corp. personally presents Keyholders, Inc., with a resolution of the Board of Directors authorizing the release of certain keys. Sure Corp. also wants Keyholders, Inc., to be liable for $200 million in the event of wrongful release. Again, Keyholders, Inc., might be willing to enter into such an arrangement, but only if it could charge a large sum for any withdrawal—both to cover the special procedures and to cover the cost of the large indemnity.

As long as the contract provisions on liability are enforced, Keyholders, Inc., can market both kinds of services and establish very different levels of security for the two customers. But if governments decide to set special procedures, all keyholders must follow to avoid liability and Quick Corp. could find itself paying for security it does not want or need.

3. *Enforcing Contractual Liability Rules*

Nonetheless, the principle also recognizes that legislation may have a role in establishing liability. Whether by contract or by legislation, the principle insists that the liability rules "should be clearly stated." The requirement is essential for the emergence of a healthy cryptography industry. If liability rules are unclear, the uncertainty will lead many companies simply to stay out of the field. These companies fear that large retroactive liability could be imposed on them years later, when it is too late to adapt their behavior to avoid the risk.

This principle therefore commits the OECD governments to avoid uncertainty in setting liability rules for those who provide cryptographic services or who hold or access keys. In theory, this situation could mean legislation spelling out liability rules in detail. But few governments, and even fewer private actors, would like this result. This dislike may explain why contracts play such a prominent role in the principle. Contracts are expected to set out fairly clear rules about liability. Governments can probably best adhere to this principle by enforcing in a straightforward way the liability provisions of contracts relating to the use of cryptography. Rather than writing an entire code of liability, legislation need only specify those circumstances in which contract is not a sufficient guide to liability. In so doing, however, governments have a special responsibility under this principle to ensure the legislation is clearly stated; the legislation must not be vague or discretionary or lend itself to the creation of surprising new liabilities.

4. *The Third-Party Liability Problem*

What are the practical consequences of favoring contract enforcement over elaborate regulatory provisions? The consequences could be substantial. Let us return to Quick Corp. and its arrangement with Keyholders, Inc. Imagine that Quick Corp. provides its encryption system not just to its employees, but also to suppliers like Supply, Inc. Supply, Inc., sends an encrypted message about its current financial condition to Quick Corp. The message is intercepted by a competitor who knows the pass phrase and tricks Keyholders, Inc., into providing the key. The competitor uses the information to steal Supply, Inc.'s customers. Supply, Inc., suffers $2 million in losses. Supply, Inc., sues Keyholders, Inc. Keyholders, Inc., offers $1,000, which is all Keyholders, Inc., owes under its contract with Quick Corp. Should Keyholders, Inc., pay $1,000 or $2 million?

This is the third-party problem in keyholding contracts. This problem can also arise when employees use their employer's encryption system to send personal messages. While Supply, Inc., seems to have a sympathetic case, to allow third-party claims that exceed the keyholder's obligations to its principal customer would destroy the keyholding industry. Moreover, on reflection, such a limitation is just. After all, by sending its confidential data to Quick Corp., Supply, Inc., was essentially relying on whatever confidentiality safeguards Quick Corp. had chosen to provide. If the form of encryption used by Quick Corp. was not adequate to protect Supply, Inc.'s data, Supply, Inc., should have used its own system, not someone else's.

The OECD's liability principle strongly suggests third-party claims against keyholders should be limited by the contract between the keyholder and the key owner. First, the principle calls for clarity in assigning liability. Second, to achieve clarity, the principle favors the application of contractual liability rules. A rule that permits third-party suits not limited by the main contract would offer neither clarity nor respect for contractual rules. A rule that enforces the main contract offers both.

This is not to say the principle leaves no scope for legislation or even international agreement on liability. The principle and the explanatory text specifically contemplate that government action may be appropriate in some circumstances. Indeed, the structure of the explanatory text provides guidance on the point. The first sentence establishes the primary importance of contractual liability rules but introduces the possibility of governmental action. The remaining three sentences describe the three areas the OECD considered appropriate for governmental rulemaking on liability.

5. *Where Is Legislation Needed?*

a. Misuse of One's Own Keys

The first appropriate area for governmental liability rules is at first glance a rather odd one: "The liability of users for misuse of their own keys should

. . . be made clear." Why should a user ever be liable for misuse of his or her own key? Can't I be as careless as I like with my own secrets? Actually, the answer is no, at least in the world of digital signatures, which this sentence almost certainly intends to cover.

When public key cryptography is used to create a digital signature, the validity of my digital signature depends entirely on whether I have kept my private key private. As long as I intend my signature to be binding, of course, I have a great incentive to keep my key private. If I leave the token holding my private key in the washroom with the access code written on the back, some stranger may loot my bank account or charge a trip to Guatemala. But suppose I'd like a free trip to Guatemala. What prevents me from buying the ticket, taking the trip, and later telling the charge company I left its token in the washroom with the access code on the back?

Digital signatures will never be widely accepted if they can be denied this easily. One answer is to enact rules discouraging negligence in the handling of private signature keys by making clear the circumstances in which users will be liable for the results. While the OECD does not require that I pay for that trip to Guatemala whether or not I took it, it does suggest a proper role for government in creating liability rules that will allow charge companies and travel agents to rely on digital signatures without worrying about later disavowals.

b. Immunity for Compliance with Access Requests

The explanatory text next turns to an area in which only governments may set the rules. The text states a keyholder should not be held liable for providing lawful access. To return to our example, imagine the National Police are investigating a Quick Corp. employee suspected of embezzling funds by generating false invoices from Supply, Inc. The National Police serve a warrant on Keyholders, Inc., for the keys to all encrypted messages between the employee and Supply, Inc. It turns out the employee is innocent but is carrying on a torrid correspondence with her lover at Supply, Inc. Due to a leak at the National Police headquarters, the correspondence ends up on a Web page entitled "America's Funniest E-mail." She sues the keyholder.

The explanatory text to this principle makes clear that the keyholder cannot be held liable for complying with the National Police warrant. This is consistent with the liability rules generally applied in the United States when third parties obey law enforcement requests for assistance in carrying out searches, wiretaps, and the like. This is an area that should be made clear. Criminals whose crimes have been exposed with the assistance of third parties are often inclined to pursue claims against the third parties. It is not in the interest of governments or keyholders if a fear of such suits deters keyholders from responding to lawful warrants.

c. Liability of Government Actors

Finally, the text identifies a third area for governmental rule-making. The text states that a party obtaining lawful access should be liable for misuse of

cryptographic keys or plaintext the party has obtained. The most obvious targets for such a rule are the government and its agents. It is true that the definition of lawful access by no means restricts such access to governments. Private litigants seeking evidence may do so by seeking the keys to encrypted files; family members may seek lawful access to the encrypted files of deceased relatives. But the confidentiality rules applying in such circumstances are probably already clear enough, or can be made so by agreement. Only governments, however, can establish the liability of government bodies and agents. This sentence urges governments to set rules for their own handling of decryption keys and decrypted material, and to enforce those rules by making sure persons injured by violations of the rules will receive compensation.

H. International Agreements

In contrast to the principle, which mentions contract and legislation as the methods for establishing clear liability rules, the explanatory text also suggests the possibility of international agreements on the topic. This is a prudent addition. The topics identified as appropriate for legislation are likely to be fruitful sources of international discussion and agreement. If digital signatures are not to be robbed of their force by spurious claims of negligence in the handling of private keys, national legislation will likely not be enough. International agreement on when to credit such claims is likely to be necessary to encourage international use of digital signatures.

Similarly, a need to agree on the liability of keyholders who provide to one government the keys of a national of another government already exists. Take the example of a keyholder in France who responds to a French government warrant by providing the keys used by a U.S. company doing business in Paris. We may assume that the keyholder could not be sued in France. Could it be sued in the United States? I asked a U.S. official a variant of that question last year, when the United States enacted a criminal statute against economic espionage. If the French government used the keys to conduct economic espionage against the American company, I asked, could the keyholder be indicted under the new U.S. law? "Why not?" said the official. Of course, the answer is plain enough. A keyholder cannot be placed in a position in which obeying one country's law is a violation of another country's. Such conflicts will require international agreement for resolution.

I. Principle Eight: International Cooperation

"Governments should cooperate to coordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade." This principle implies in its first sentence that nations have an obligation to cooperate and to coordinate in making cryptography policy. This principle does not require that all the OECD

members adopt the same policy, or even a harmonized policy. But the principle does call for continued communication and an effort to ensure each nation's cryptography policy is capable of functioning with the policies of other nations. The second sentence contains a tough admonition to avoid the use of cryptography policy to create unjustified obstacles to trade, and even to remove existing obstacles created by cryptography policy if the obstacles cannot be justified.

This sentence obviously begs the question of how such obstacles can be justified. The language is borrowed from international trade law, in which what is unjustified has been defined by usage. The most likely interpretation in this context is that cryptography policy should not be used as a pretext to exclude or to discriminate against foreign products. The principle is not intended to override national security or law enforcement policies if applied in good faith, and clearly does not prohibit Wassenaar export controls, since several major OECD members maintained such controls on cryptography when the Guidelines were adopted. On the other hand, as one astute delegate has pointed out to me informally, a world of difference exists between unjustified and unjustifiable obstacles. By choosing the former language, the OECD called upon member nations to proffer understandable justifications for their policies on cryptography. Like the recommendation that member nations state their cryptographic policies clearly and publicly, this principle calls for an end to subterranean cryptographic policy making.

The explanatory text adds only a little to the concept of unjustified obstacles, but does focus on avoiding obstacles in two contexts. The explanation focuses first on obstacles to global electronic commerce. Because cryptography is thought to be particularly valuable in fostering global electronic commerce, this focus may prove important. In addition, the text makes clear that the principle applies specifically to unjustified obstacles to the international availability of cryptography. This opens the door to requests that nations justify their export control regimes as well as their import and domestic policies.

The text also elaborates on international cooperation in three contexts. First, the document notes lawful access across national borders may be achieved through bilateral and multilateral agreements. Indeed, in the classic case of lawful access across borders—one nation seeking keys held in another nation—how access could be achieved except through agreements between the two nations concerned is hard to see. But lawful access includes access by private parties for private purposes, and such access can occur across borders without any governmental involvement whatsoever. That fact may explain why the text says simply that such access *may* be achieved through government-to-government agreements.

Second, the text offers strong guidance to those nations that develop domestic key management systems. Without endorsing the development of such systems, the text advises that such systems must allow international use of cryptography. This "must" is apparently intended not as a command but as a statement of fact: that markets will not tolerate key management systems that do not allow

international use of cryptography. But it seems clear the OECD itself also strongly favors systems that fulfill this market requirement.

Third, the text states nations should not impede the free flow of encrypted data passing across their national territory merely on the basis of cryptography policy. This principle is borrowed from a strong ITU rule against actions impeding the flow of international communications across the territory of a member state. This policy against impeding the flow of encrypted data is limited to data transiting a particular country. That is, when encrypted data crosses country A on its way from country B to country C, the cooperation principle calls on country A not to impede the flow of data between countries B and C.