
OCCASIONAL PAPERS FROM
THE LAW SCHOOL
THE UNIVERSITY OF CHICAGO

NUMBER 38

**THE ROLE OF PRIVATE
GROUPS IN PUBLIC POLICY:**

CRYPTOGRAPHY AND THE NATIONAL
RESEARCH COUNCIL

BY KENNETH W. DAM



THE LAW SCHOOL
THE UNIVERSITY
OF CHICAGO

THE ROLE OF PRIVATE GROUPS IN PUBLIC POLICY:

Cryptography and the National Research Council

BY KENNETH W. DAM^{*}

An academic growth area has been the study of interest group politics in determining public policy outcomes. We all know that many decisions in the Congress and in the Executive Branch are not the outcome of reflection and deep study by public policy wonks. Nor are these decisions the outcome of dispassionate debate on the political hustings and on the floor of Congress. Rather the clash of interest groups in the public arena and perhaps even more in the more sheltered corridors of power are frequently decisive. It is a story of lobbying, political contributions, and door-opening political influence.

Sometimes issues come along, however, that can only be resolved by serious and sustained study. One thinks immediately of the 1983 Greenspan Commission that saved social security for a few decades and that is likely to be reincarnated soon under another name for the same purpose. In such cases the crucial decisions have to be vetted quietly among experts and serious generalists devoted to better public decisions.

Short of serious government commissions of the Greenspan type, there are ways to assure that at least such serious public debate as exists is informed by the best fact-gathering and analysis available in the private sector. Where science and technology play a role in public decisions, one institution that can and does frequently play that role is the National Research Council ("NRC").¹ The NRC's

"The Role of Private Groups in Public Policy" is adapted from a presentation made to the Presidents' Circle of the National Academy of Sciences and the Institute of Medicine, Washington, D.C., November 21, 1996. Copyright © 1996 by Kenneth W. Dam

Copies of *Occasional Papers* from the Law School are available from William S. Hein & Company, Inc., 1285 Main Street, Buffalo, New York 14209, to whom inquiries should be addressed. Current numbers are also available on subscription from William S. Hein & Company, Inc.

^{*} Max Pam Professor of American and Foreign Law, University of Chicago Law School; Chair, Committee to Study National Cryptography Policy, National Research Council. This paper is adapted from a presentation made to the Presidents' Circle of the National Academy of Sciences and the Institute of Medicine, Washington, D.C., November 21, 1996.

¹ The National Research Council is the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the U.S. government and public.

study on Cryptography's Role in Securing the Information Society is an example of a study that has played a significant role in the making of public policy.² Although the key issues are not primarily technological, the fact that they concern a technology most people find esoteric gave the NRC a comparative advantage in explaining the technology and laying bare the underlying non-technological issues for a public audience.

I. THE CLIPPER CHIP AND THE NRC REPORT.

The cryptography issue had been debated largely behind closed doors in the Executive Branch. But there were sharp differences in opinion and interest among the various departments and agencies concerned. Although the Executive Branch process resulted in a public proposal early in the Clinton Administration (after a similar proposal had been rejected by National Security Advisor Brent Scowcroft late in the Bush Administration), this proposal—usually called the Clipper Chip proposal—met a storm of public protest and technical criticism. The intensity of the public reaction caught the Administration offguard and in any event revealed a sharp difference of values held by different parties in the debate—a phenomenon that should not be surprising in view of the conflicting law enforcement, national security, privacy, civil liberties and other interests at stake.

Perhaps more worrisome, the reaction of some parts of the public revealed a deep mistrust of government and an unwillingness by some partisans on several sides of the debate to take the concerns of others in the debate seriously. Yet the Administration seemed unable either to put its proposal into operation or to modify it in a way to calm the criticism. In response, the Congress in the Defense Authorization Act for Fiscal 1994 mandated an NRC study of national cryptography policy to be financed out of Department of Defense appropriations. This mandate, it should be noted, was much broader than just a study of the Clipper Chip proposal, thereby enabling the committee to examine

the area from first principles and to make proposals encompassing the entire field, rather than just the specific area encompassed by the Administration's still-born proposal.

The NRC study got underway in the fall of 1994 and was made public in May 1996, receiving wide media and trade press attention. The study made recommendations that differed from the Administration's public position in substantial ways.

Virtually all of the press commentary was favorable. And the study was well received by a Senate Committee before which I, as committee chair, and Herbert S. Lin, the study director, testified in June. More significant than the public reaction was that within the Executive Branch. The key officials were well aware of what was coming because we had briefed them in detail prior to the public release of the report. In May shortly before the report appeared, the Administration floated a modification of their then-position (which had already been modified somewhat during the course of the study). This May modification moved in the direction of the NRC study and could be interpreted as an effort to undercut the criticism implicit in the forthcoming report. Moreover, the Administration again modified its position in October, moving in the direction of the NRC recommendations and explicitly citing the NRC report in support of its new position.

II. A QUICK PRIMER ON CRYPTOGRAPHY.

A short introduction to the basic concepts in cryptography policy may be helpful to some readers. Others may prefer to skip directly to Part III below.³

At the simplest level, cryptography involves the scrambling of messages so that they cannot be understood by anyone other than the intended reader or listener. We call the technique for scrambling the message encryption and that for converting it back to the original message decryption. Otherwise put, encryption turns plain text into cipher text, and decryption turns cipher text into plain text.

Cryptography does so by converting ordinary language words or sounds into an unreadable flow of

² Kenneth W. Dam and Herbert S. Lin (eds.), *Cryptography's Role in Securing the Information Society* (National Academy Press 1996) ("NRC Report").

³ Those seeking greater detail on cryptography, without however entering the realm of mathematics, should consult id., Appendix C, at 364.

numbers and letters through the use of an encryption algorithm. In addition to the algorithm, which can be used by an unlimited number of people, a particular user will encrypt his message through use of an encryption key that is unique to him. Just as the lock in my front door can be secured only by my key and unlocked only by my key, so too I can keep my message secure against all but the intended receiver by using my own personal key. Once my message is encrypted using my key, only the right key will decrypt it. If someone uses a different key to try to decrypt it, he gets garbage. And just as I will not want just anyone to have a copy of my house key, so too I will want to pay attention to what is called “key management.” After all, if the encryption key falls into the wrong hands, my messages will not be secure.

One way to achieve this security is to make special arrangements to transport the secret key to the intended recipient of the message by, say, secure courier. High technology companies and financial institutions that use encryption widely thus have to pay great attention to key management of their secret keys.

Two decades ago a second technique was developed for transmitting the secret key. This was called public key cryptography. This method of sending secret keys was a byproduct. The principal purpose of public key cryptography is to send decrypted messages to people one does not even know. Today for reasons of speed and efficiency, public key cryptography finds its greatest use in transmitting a secret key to a party located at a distance from the sender of the encrypted message, and the recipient then uses the secret key, which he has decrypted for his own use, to decrypt the main message and other messages using the same secret key. Use of public key cryptography to transmit the message means that a sender can change the secret key with every message, and therefore the sender does not have to trust the first recipient not to use the secret key to decrypt a second message to another party.

The beauty of public key cryptography is that if I am sending you a message, I can use your public key that you can give to the entire world, but only you can decrypt the message. One can easily envisage a world a few years hence when there will be the equivalent of telephone books listing everyone’s public key, and this will facilitate sending confiden-

tial messages to people one does not trust and may never have met. The fact that we do not yet have in place a public key infrastructure that would allow this kind of security in all messages is one example of how national cryptography policy is thus far almost hypnotically focused on the dangers of cryptography, not its potential benefits.

Suppose for a moment we put ourselves in the place of some third party who wants to read an encrypted message between two other parties. There are basically only two ways to go about doing so. One is to analyze the message using a variety of techniques widely practiced by governments and perhaps some high tech criminals. One can use a variety of statistical techniques for doing so (such as relying for example on the fact that approximately 14% of the words in English-language texts involve the letter “e”). Some cryptographic applications are vulnerable to decryption because they are poorly implemented and therefore are not as strong as they appear to be. In that event, analytical techniques may uncover the vulnerability and facilitate decryption.

If analysis fails, then the only alternative is so-called brute force decryption. This term refers to the decryption of a message encrypted with a known algorithm by trying each possible key. The number of possible keys depends on key length. Where the key length is 10 bits, then there are by definition 2^{10} possible individual keys, and it would be trivial using a computer to try each possible key. An important point is that adding one more bit doubles the number of possible individual keys.

In the discussion that follows, I shall refer to two common key lengths, 40 bits and 56 bits. Encryption using a 40-bit key may be impenetrable by amateurs but is today regarded as weak cryptography because an expert with even one desktop computer can with enough time decipher such a message.⁴ But a 56-bit key is regarded as strong cryptography because of the doubling-per-bit phenomenon. A 56-bit key is roughly 65,000 times as powerful as a 40-bit key and therefore takes in principle 65,000 times as much time on any given computer or set of computers to decipher by brute force.

⁴ Id. at 287 reporting a successful brute force attack in eight days using a single computer workstation.

The reader may ask why emphasis should be placed on the number of bits. We will see shortly that it is presently unlawful, with certain exceptions, to export from the United States an encryption device or program stronger than 40 bits, but the NRC report recommends that this limit be increased to 56 bits, and the Administration proposes to do so as of January 1, 1997. Under the Administration's newest proposal this right to export 56 bit cryptography will be available for companies that commit to certain undertakings having to do with "key escrow" or, to use the new Administration phrase, "key recovery."

"Key escrow" a.k.a. "key recovery" is the final concept that needs explanation before we plunge into the public policy problem. The term refers to an arrangement under which a copy of the key is deposited with some third party (now often known as a "trusted third party") so that it can be recovered by the depositor (hence the new term "key recovery"). Alternatively, some other party, such as the FBI with a court order, can obtain the key without the knowledge of the key depositor for the purpose of wiretapping. The term "key escrow" thus refers to the fact that the third-party key holder will release it only on conditions specified in law, just as a bank might hold a real estate deed until entitled to release it under the terms of an escrow agreement.⁵

With these terms and concepts in mind, let us now consider why cryptography presents a powerful public policy challenge. After all, cryptography has been around for thousands of years.

III. SOME INTERESTS AT STAKE.

In an electronic age with packaged software and increasingly capable semiconductors, cryptography is potentially available to every person who talks on a telephone, sends a fax, or communicates by e-mail. Indeed, it can be built into hardware or software so that the user need not even be aware that his message is encrypted. So too for the recipient.

⁵ Proposals for key escrow normally envisage that the key will be broken into two or more parts in order to give more confidence that the full key will not accidentally or unlawfully be made available to anyone except as envisaged under the particular key escrow arrangement and the wiretap statute.

Moreover, in an era where we not only communicate privately by electronic means but where vast sums of money are transferred electronically and where many of our most critical national information systems and networks function electronically (from the public switched telephone network to the air traffic control system to the FedWire system that transfers more than a trillion dollars a day), we are increasingly vulnerable as a society to being brought to our collective knees by electronic vandals enjoying their prowess and by rogue states engaging in electronic warfare. As former CIA director John Deutch said, the question is not whether we will experience some kind of electronic disaster in one or more of these critical national systems and networks, but when.⁶ Cryptography alone cannot deal with these kinds of challenges, but it is an indispensable part of any solution.

Cryptography, with all of its modern implementations, is a powerful technology. But like all technologies it can be used for good or for evil. It can be used to serve society or to harm it, and it will be used for both purposes by different groups. The role of cryptography policy should thus be to promote the good uses of cryptography while limiting those uses that threaten society. To give this abstract calculus some flesh and bones, let us consider first the two main interests threatened by more widespread use of cryptography—law enforcement and national security.

Law enforcement can be harmed in primarily two ways. First, when the FBI and other law enforcement agencies, operating lawfully with requisite court orders, wiretap a telephone line to catch a criminal and perhaps even to preempt a crime, they will not succeed if the telephone call or fax transmission has been encrypted. The results could be catastrophic. The attempt to blow up the World Trade Center illustrates the potential stakes. Second, law enforcement authorities operating under a search warrant may find a treasure trove of evidence on a computer hard drive or on a floppy

⁶ John Deutch, responding to questions from Senator Sam Nunn, Permanent Investigations Subcommittee of the Senate Governmental Affairs Committee (June 25, 1996). Deutch also stated: "The electron is the ultimate precision-guided weapon." "Prevent a High-Tech Pearl Harbor," *Chicago Tribune* C18 (June 30, 1996). For a description of vulnerabilities, see NRC Report, Box 1.8 at 34, and Appendix I at 455.

disk, but they won't find anything useful if the material is encrypted.

National security interests can also be seriously compromised by encryption. Today our government may be the only superpower, but our ability to know what is going on in the world in the security realm depends on national intelligence techniques for "listening in" on our enemies and potential enemies, including foreign companies that supply and support them. Signals intelligence, or SIGINT, may well be the most important source of foreign intelligence for our national policymakers. Ubiquitous encryption abroad could undermine our ability to provide those policymakers with the information they need to make wise decisions and to avoid disastrous mistakes based on inadequate knowledge of the "facts on the ground" abroad.

Note that both law enforcement and national security are concerned about cryptography becoming ubiquitous abroad. Consider, for example, terrorism and drugs.

If one thinks only of law enforcement and national security interests, particularly in this conventional way, it is easy to decide that national policy should restrict the use of cryptography and particularly its free export. But there are other interests. And they are equally legitimate and weighty.

In a free society individuals expect and are entitled to privacy. Business has a need to protect its intellectual property in the form of trade secrets, of sensitive business plans (such as proposed competitive bids), and of a host of other kinds of proprietary information. And we all have a stake in protecting our critical national information systems and networks on which we increasingly rely.

One of the key findings of our report is that all of these interests are legitimate, and there are conflicts among them. To be specific, some law enforcement and national security interests tend to conflict with our interests in individual privacy, protection of business, and the inviolability of our critical national information systems and networks.

Nevertheless, in our examination of law enforcement and national security interests, we made several important findings. We found that, legitimate and weighty as those interests are, it would be wrong to take the worst-case view that those interests will be so seriously compromised that the spread of cryptog-

raphy should be resisted at all costs and that other interests should be subordinated.

Take law enforcement for example. While there are instances in which cryptography has interfered with wiretapping and perhaps more instances in which it has prevented the reading of computer files, law enforcement officials were not able to demonstrate to us that this is by any means a regular occurrence. Perhaps it will be in the future, but not now. Moreover, so far as computer disks are concerned, even the Clipper Chip proposal of the Administration did not purport to bar the use of cryptography to protect computer files. It would have reached only communications. Nor are the key escrow proposals of the Administration relevant to the encryption of files on, for example, the hard drive of one's own computer.

More crucial, however, is the way in which we assess what the law enforcement interest really is. On reflection, I think it obvious that the purpose of law enforcement is to reduce the crime rate. One way to do so is to catch criminals and punish them. Deterrence works. But it is also true that in our increasingly electronic society, where more and more business is done electronically, the rate of computer-based crime is rising rapidly. And we have yet to lay secure foundations for broadscale electronic commerce, potentially a revolutionary economic development for which all elements are already in place, save protection against crime.

Today financial institutions are particularly vulnerable, even though they don't like to talk about it for fear of encouraging more crimes. But the ability of a group working out of St. Petersburg, Russia, to penetrate the Citibank system in the United States and to extract cash by electronic means illustrates the possibilities.⁷ The ability of hackers to penetrate Defense Department computers some 250,000 times in one year equally illustrates the potential.⁸ Almost half of 200 large companies responding to a survey questionnaire admitted suffering electronic break-ins in the last 12 months.⁹ Cryptography, it seems obvi-

⁷ Id. at Box 1.2 at 23. For other examples, see id. at 470.

⁸ "Report Warns on Security Threats Posed by Computer Hackers," *New York Times* A22 (May 23, 1996).

⁹ "Firms are Hurt by Break-ins at Computers," *Wall Street Journal*, p. B3 (Nov. 11, 1996).

ous, has to be part of any solution to this challenge.

Yet the FBI and other law enforcement authorities have a more immediate short-term bureaucratic interest in solving crimes the public knows about. This is particularly true of the FBI, which is facing a public relations crisis of the first order in view of a series of highly visible miscues in the past few years. To fail to solve a major crime that had gained national attention could be a public disaster for the FBI. But the FBI's immediate interest in solving high-profile crimes is not the same as the nation's interest in preventing crime—especially if measures to suppress cryptography were to lead to rapidly escalating computer-based crime in our electronically vulnerable society.

The same kind of analysis of national security interests leads to a related conclusion. In the post-Cold War world what exactly are our national security interests that would be negatively affected by more widespread use of cryptography abroad? Let's remember that even more stringent export controls could not prevent major foreign governments from using high-strength cryptography to safeguard their national secrets. Rather the national security concern is that in a world of increasingly ubiquitous cryptography, our foreign intelligence agencies will lose access to many kinds of information that are now accessible.

While we as a nation would lose a lot if we did not have access to the information we derive from such sources, we could well lose even more if we became more vulnerable at home. Part of the reason that the United States has superpower status is that our companies lead the world in most technologies. If national policy makes their intellectual property more vulnerable, we as a society become more vulnerable. We know that Russia has publicly declared that its national policy is to improve its economic and military capability by using intelligence methods to obtain proprietary technology.¹⁰ The French government is doing the same for the benefit of its own companies, though without admitting it.¹¹

¹⁰ "Economic Espionage Rising, FBI Director Tells Congress," *Washington Post* D11 (Feb. 29, 1996); "Yeltsin Orders Targeting of West's Hi-Tech Secrets," *The Guardian* 13 (Feb. 8, 1996).

¹¹ *Id.* at Box 1.7, at 32.

Similarly, if the failure to use cryptography makes our critical national information systems and networks more vulnerable, our national security is threatened. I hope we shall never see the day when the world's only superpower is humbled by a fourth rate power using a few computer experts to disrupt our ability to fly our airliners or to operate our stock markets or our banking system, even for a few days. Information warfare need not be about one more weapon in an actual war. It may be the poor country's alternative to actual war as a way of deterring our country from carrying out our policies.

IV. THE DOMESTIC EFFECTS OF EXPORT CONTROLS.

One may well ask, as we on the committee asked ourselves, how existing export controls can make us more vulnerable here at home to electronic crime and to information threats that reduce our national security. After all, export controls limit exports, not domestic use. We found, however, that existing export controls have an unintended negative loopback effect on the domestic availability of strong encryption and thereby make us more vulnerable to computer-based crime and to information warfare attacks.

To understand that finding, consider the case of a typical U.S. multinational corporation doing extensive business abroad. Most such corporations want to do business abroad in the same way they do it in the United States. They want to be on-line with their suppliers and customers. This is especially true in high tech manufacturing industries, where American assembly plants buy components from around the world. It is precisely in the same high tech industries where our U.S. technology is most vulnerable to appropriation by foreign competitors and others who seek to profit by penetrating our multinationals' communications. Similarly, competitors may hope to learn confidential business plans, such as proposed competitive bids.

Someone who knows the details of export regulations might well ask what there is to worry about since U.S. corporations, as an exception to the general export prohibition, are entitled to export as strong cryptography as they wish for their own use. The problem is that they can only use weak cryptog-

raphy—that is, 40 bit cryptography—when they are on-line with their foreign suppliers and customers.

This limitation on the scope of the U.S. corporation exception is critically counterproductive in two ways. First, U.S. proprietary technology and business plans are ready targets for foreign penetration when they are shared on-line under only weak cryptographic protection. Second, and even more important, many corporations will not find it cost-effective and in some cases not even technically feasible to use two systems, one inside the corporation and another in communications with their foreign suppliers and customers. It is this latter effect on a U.S. corporation's internal communications that is a negative loopback effect because it may extend all the way to a U.S. company's communications within the United States. So export controls can, and in many cases doubtless do, tend to cause some U.S. businesses to use weak cryptography at home, thereby leaving themselves open to all manner of rivals, scoundrels and crooks.

This part of our finding focuses on the demand for cryptographic equipment and software. The same negative loopback effect can be found on the supply side.

It is expensive for software firms producing packaged software for e-mail, spreadsheets and business applications to produce two versions, one for domestic use and one for export. The result is that they may produce only one version, the weaker exportable version. To be sure, the cost of two versions may not be prohibitive for the larger software companies. But they may still be disinclined to produce two versions, perhaps for marketing reasons. And the thousands of smaller, newer software specialists and startups may find that they have neither the staff nor the time to do so. Integrating cryptography into complicated programs is not trivial. And being first to market is usually essential to success.

To the extent that software firms decide not to produce two versions, they may elect to produce the weak version. Such decisions reinforce the negative loopback effect of export controls. Alternatively, and perhaps even worse, they may elect to produce the strong version, in which case they abandon the export market.

The election of a software firm to abandon the export market is not a victory for our government.

Foreign customers are no less sophisticated about their electronic exposure to hackers and criminals than U.S. customers, and both are likely to demand strong cryptography in their software applications when they can find it. So the question is not just one of lost sales and hence lost export earnings and fewer jobs. Such losses may not be obvious or at least not measurable in the short run. But in the long run you can be certain that, if export controls lead to widespread decisions by our software firms to limit themselves to the U.S. market, the result will be that the U.S. software industry will gradually lose its present dominance of the principal packaged solutions in the world market.

Plenty of good software firms can be found abroad, especially in Europe, and overly stringent export controls give them a golden opportunity to catch up with the U.S. software industry. Fortunately, there are not yet so many high quality software applications incorporating strong cryptography at area available from first-rank foreign vendors. Certainly such integrated applications are not yet available in off-the-shelf shrink-wrapped versions. In that sense, the cat is not yet truly out of the bag. The fact that there are lots of strong cryptography programs circulating abroad is not the determinative element because, again, integrating powerful applications with strong cryptography is not trivial. Even if U.S. firms produce two versions (strong for home and weak for export), nearly the same effect may result because foreign customers are unlikely to be satisfied with what they view as a second-class product. They want the "North American version" and, not finding it, they are likely to hunt for an alternative abroad.

If it is true that overly stringent export controls provide a free take-off zone for foreign software firms to gain a sizable share of world markets, that will be no victory for U.S. national security. It was our judgment that our national security is advanced by the continuing first-rank position of the U.S. software industry.

One final point: There was a second kind of negative loopback effect that the Administration failed to focus on (and that I believe they are still not focusing on sufficiently). All of the concentration within the Administration on the deleterious effects of widespread cryptography on law enforce-

ment and national security led the Administration to fail to give much attention to the need to promote computer and communications security, including that of our critical national information systems and networks.

To the extent that this vulnerability was addressed, it was treated mostly as a question for a few specialized agencies of the Federal government. The National Security Agency has a responsibility for computer and communications security in the classified world, the National Institute of Science and Technology in the Commerce Department has a similar responsibility for sensitive but unclassified communications within the government, but no one in government has a responsibility for computer and communications security in the private sector as a whole. What attention there is paid to these matters is on an industry-by-industry basis. For example, the Federal Reserve Board is presumably responsible to some degree for the security of the banking payments systems, both public and private. Insofar as the vulnerability involves private sector systems, the governmental allocation of responsibilities simply ignores the problem.

Yet cryptography has to be a crucial element in solutions to those private sector systemic vulnerabilities. Even if the government cannot by itself bring about solutions, it has a leadership responsibility that it is not meeting because it is focused on the negative aspects of cryptography.

V. THE RECOMMENDATIONS.

My summary thus far has focused on a number of background facts and a few crucial analytical points. Let me now quickly run through our recommendations before turning to an analysis of the impact of our report on the Washington policy process.

Our first three recommendations were rather general, but they reflected our views on what was wrong with the policy process:

Our first recommendation was that “no law should bar the manufacture, sale, or use of any form of encryption within the United States.”¹² That was, of course, the Administration position, but the main reason that we made that recommendation was the

recurring rumors that the FBI and the Justice Department leadership were prepared to come back to the Administration, or perhaps even go directly to the Congress, to demand an absolute bar on non-escrowed encryption if they felt it necessary to protect their interests. In my view at least, not only would a ban be wrong, but even to propose it would be a foolish, perhaps tragic mistake of policy formation. Such a ban would be mostly symbolic because it could be easily circumvented technically. Moreover, it would raise a sufficient number of Constitutional issues as to simply inflame the controversy unleashed by the original Clipper Chip proposal.

The second recommendation: “National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and governed by the rule of law.”¹³ This rather grand language was designed to say that the policy process had become moribund. Trying to achieve a positive outcome through discussions in closed rooms in the Executive Branch had produced proposals but no action. Essentially no change had been made to the export rules since 1992. In the face of the well-known “Moore’s law” that computer power doubles at least every 18 months, the policy process had reached stasis.

The Administration was facing a policy crisis. What was needed was a way of reaching a national consensus on a coherent national policy toward cryptography—a consensus not just within the Executive Branch but, if it were to be implemented, a consensus with the outside stakeholders as well—the software industry, those concerned with computer security, and the civil liberties community. There is only one way to reach a national consensus, especially after controversy has hyped the atmosphere, and that is through public debate. Congressional involvement is thus an asset rather than a liability.

Recommendation three: “National cryptography policy affecting the development and use of commercial cryptography should be more closely aligned with market forces.”¹⁴ The Clipper Chip was invented and its roll-out was planned exclusively in government. The same was mostly true of its key escrow proposals. So it is small wonder that the private sec-

¹² Id. at 303 (emphasis added).

¹³ Id. at 304.

¹⁴ Id. at 305.

tor found faults—true faults, not just a not-invented-here reaction. Moreover, a failure to use private sector input from our computer and software industries, two of our fastest moving, most inventive industries, verges on arrogance and foolhardiness. The solution should be to harness, not to flout market forces. At a time when most governments in the world were finally learning that lesson (witness the worldwide deregulation and privatization movement), the U.S. government was failing to apply the same lesson.

The heart of the report is to be found in recommendation four: “Export controls on cryptography should be progressively relaxed but not eliminated.”¹⁵ We were emphasizing liberalization, but for the time being at least a gradual approach. In short, we wanted to avoid the negative loopback and other deleterious effects of the Administration’s standpat position without going so far as to undermine law enforcement and national security interests.

This approach would assure that software firms could sell a single product here and abroad, increase the availability of good cryptography in the United States by eliminating the negative loopback effect, and solidify the world leadership of the U.S. software industry. And it would buy time for U.S. law enforcement and national security to adjust to new technical realities.

Despite the moderate nature of this general proposal, our implementation recommendation galvanized the attention of U.S. policymakers. We proposed to allow liberal export of 56-bit DES-based products.¹⁶ To some in government, this was a startling recommendation because, as explained above, 56-bit encryption is 65,000 times stronger than 40-bit encryption, the existing ceiling on free exportability. But we chose DES because it is a recognized standard and there are existing products available from many firms that implement it. DES is well-known, well-analyzed, and widely accepted commercially. Specifically, most businesses consider 56-bit DES adequate for their security needs today. And there are no well-known existing products between the existing 40-bit level and our proposed 56-bit level.

For those who argue that there should be no

export controls at all, at least on shipments to friendly countries, I should emphasize that we were not saying that DES is strong enough for every application in every industry. Nor were we saying that it will remain strong enough indefinitely. On the contrary, we were saying that for the present it represented the first step in gradual relaxation. The pace of relaxation would depend on many factors, not least the pace of computer power growth, and perhaps the pace of decryption technology in the private sector.

We recognized that university professors and graduate students throughout the world were experimenting with new methods of cracking codes, and even the progress being made during the period we were meeting suggested that the encryption world could be facing surprises at any moment.¹⁷ Indeed, Recommendation 4.2 specifically recognized the desirability of allowing export of even stronger encryption than DES to firms “willing to provide access to decrypted information upon legally authorized request.”¹⁸

Recommendation five shifted the attention to the importance of taking other kinds of “steps to assist law enforcement and national security agencies in meeting the new technical realities of the information age.”¹⁹ Much can be done through R&D to help the FBI deal with new communications technologies. Indeed, even if there were no such thing as encryption, the modern communications technologies of packet switching and dynamic routing may soon mean that the FBI will not be able to interpret wiretaps without the assistance of telephone companies in assembling full messages. Similarly, the government needs to push the use of cryptography in so-called non-confidentiality applications to protect critical national information systems and networks like the air traffic control system.

Finally, in recommendation six we addressed the need for the government to promote information security in the private sector.²⁰ After considerable discussion, we decided not to tell the Administration how to move the boxes around on its organiza-

¹⁵ Id. at 307.

¹⁶ Id. at 312.

¹⁷ Id. at 390-394.

¹⁸ Id. at 317.

¹⁹ Id. at 322.

²⁰ Id. at 335.

tion chart, but rather to emphasize the urgent priority of addressing the question of who was in charge. Today no one is in charge.

The most newsworthy aspect of the report, other than the DES recommendation, was a refusal to endorse the Administration's proposed system of escrowed encryption, although a sub-recommendation does urge that the "U.S. government should explore escrowed encryption for its own uses" to gain experience.²¹ What that means in plain English is that we were opposed to the ongoing Administration attempts to impose key escrow on the private sector. The Executive Branch has plenty of opportunities to experiment with and improve key escrow mechanisms within the government and potentially in government communications with, say, defense contractors. Until that kind of work has been done, it would be highly risky to require key escrow throughout the country.

Although we believed and stated that key escrow is a promising technology, we also agreed with critics that it is an unproven technology whose precipitate implementation by government fiat could be disastrous. The fundamental reason is that introducing an escrow agency simply introduces a new point of vulnerability. Most people are very careful about giving keys to their house to strangers, yet key escrow requires exactly that for encryption keys. Although key escrow agents would no doubt be licensed and many banks and similar institutions would perhaps compete for the role, they inevitably will have to rely on human beings. Humans are regrettably vulnerable to bribery and coercion.

Any escrow arrangement used on a large scale would, moreover, almost inevitably involve some kind of on-line arrangement for receiving keys and perhaps for making them available to law enforcement agencies (with a warrant to be sure). Any machine that is on-line is potentially vulnerable to outside penetration. With expert attackers, so-called firewalls may be just as good protection as the Maginot Line proved to be for France. Moreover, unlike someone holding the key to a neighbor's house, a key escrow agent would hold thousands upon thousands of keys, raising the possibility of

"open Sesame" access to a vast number of computers and communications devices.

Another factor was that we felt that key escrow could not be implemented without legislation. Surely the liability of key escrow agents would have to be specified and perhaps even limited in view of the potentially astronomical losses in, say, the banking industry. Neither aspect of liability could be specified through regulations without some kind of framework in legislation. That, by the way, is another reason why it is a mistake to think that cryptography policy can be implemented without involving the Congress. In short, we should proceed with all due caution and prudence in the development of key escrow mechanisms. This recommendation was met, I am sure, with disappointment in those parts of the Administration who were hoping for some quick technological fix to square the policy circle.

VI. LESSONS LEARNED.

Prior to public release, we briefed the report to all important players within the Administration and not just to their staffs. My impression from those private briefings was that the reaction to the report largely reflected the going-in positions of the various departments and agencies. Disappointment was freely expressed in some circles. At the same time I had the distinct feeling that some inside players secretly welcomed our recommendations, if for no other reason than they saw them as a way of breaking the policy logjam within the Administration.

The public release of the report received considerable attention in the major newspapers, on CNN and National Public Radio, and in the trade press. The report and recommendations were on the whole quite well received.²²

The Administration did not directly criticize the report, even though it was at odds in major ways with declared Administration positions. At least one Administration insider did background the press with the observation that they after all bore the

²¹ Id. at 328.

²² I can think of only one major public rejection of our approach and that was an editorial in the *Washington Post* which had little apparent influence. "Global Village Cops," *Washington Post* A18 (June 10, 1996). For an analysis and rebuttal, see Kenneth W. Dam and Herbert S. Lin, "The Crypto Wars," *Washington Post* A17 (June 23, 1996).

responsibility and therefore might view the dangers to law enforcement more seriously than we. Not surprisingly, most members of Congress addressing the issues welcomed the report, and those who may have been more reserved about it kept that reaction to themselves.

In short, the report generally received little but accolades. Indeed, the Administration's later changes in position (which I shall outline shortly) specifically relied on "the NRC report," even in one instance in a White House release involving a change that we consciously did not recommend. That change involved the transfer of the licensing function from State to Commerce, a change that had been advocated by many private sector firms. But we had consciously refrained from recommending it because we believed it to be mostly cosmetic. Rather we had merely advocated a streamlining and increased transparency of the licensing process to reduce the long delays that were themselves proving a disincentive to U.S. exports.²³ To the extent that the transfer would be a cosmetic change, it would be somewhat deceptive in implicitly promising liberalization without delivering it. The important point, however, is that the White House seemed to feel that the NRC report was so important that they could gain support by relying on it.

How is the widespread public acceptance and endorsement of the report to be explained? Let me put to one side the thought that its inherent quality and merit provides the explanation. That is rarely enough in Washington—indeed, sometimes not even relevant. The libraries are full of outstanding public policy reports that were never read nor referred to after the day they were released.²⁴

I believe four factors account for the warm public reception. The first was that despite the seemingly intractable conflict in objectives and values presented by the long-running dispute, we had a unanimous report.

²³ NRC Report 321.

²⁴ Nonetheless, I believe that not just the analysis but also the sustained quality of the presentation and writing of the NRC Report deserve recognition. For that the committee has the outstanding and extraordinarily dedicated and hard-working NRC staff to thank. A 600 plus page book filled with great detail and ranging over a wide spectrum of technological, historical and policy questions is not something that can be produced by a committee of part-timers.

The second factor was that this unanimous report came from sixteen different people who were experts in their respective fields. We consciously chose people from each relevant field of expertise and viewpoint. The committee included, as I noted in my preface to the report, "individuals with extensive government service and also individuals with considerable skepticism about and suspicion of government; persons with great technical expertise in computers, communications, and cryptography; and persons with considerable experience in law enforcement, intelligence, civil liberties, national security, diplomacy, international trade, and other fields relevant to the formation of policy in this area. Committee members were drawn from industry, including telecommunications and computer hardware and software, and from users of cryptography in the for-profit and not-for-profit sectors; serving as well were academics and think-tank experts." We tried to pick a person in each of those constituencies who was so well grounded in his or her field, and had such a high level of attainment within it, that members of each such constituency would be led to conclude, rightly I believe, that all members of the committee (including those they had never heard of) were of equal quality.

Let me tie factors one and two together. How did we achieve consensus about a highly controversial subject with sixteen so diverse personalities, none of whom could be considered a shrinking violet? The answer lies in our working methods. We met together for 23 days of plenary sessions; while there were individual absences, they were definitely the exception. And many of us spent additional days in subgroups and meeting with outsiders. During our 23 days together as a group, we talked out each and every issue at length. Moreover, we together met with each government agency and each interest group with knowledge or relevant points of view, and with many individual experts as well.

Surely there was not a single member who came out of that process with exactly the same views he came in with. In my view, committees cannot make convincing driving recommendations that will command respect if they merely meet to paper over their entering differences. Unfortunately, that is what happens in most public committees and study groups, and the result is, as Churchill put it, "a pudding."

The third success factor derives from the second. We heard out every party with something to offer. Indeed, thirteen out of the sixteen of us received the highest level government security clearances, and met at length in classified session with our most qualified and highest ranking officials and civil servants. In my view, the intelligence community delivered on its promise to tell us everything that was in any way relevant to our inquiry.

The fourth factor is related to this last point. We concluded that we were able to say, based on this experience with the intelligence community, that it was not necessary to have access to classified information in order to make a judgment about the proper disposition of the public policy issues. To my knowledge, no one in government has disputed that conclusion. This conclusion lifted the fog that had obscured public discussion because, so often, the impression was left with outsiders that they were being told by government officials that "if you knew what we know you would agree with us."

VII. THE ADMINISTRATION'S POLICY RESPONSE.

I have left for last the Administration's subsequent policy changes. I believe our report had a major impact in bringing about those changes, although perhaps more as a galvanizing event than through its precise recommendations.

First, as previously mentioned, a proposed change was floated just a few weeks before our report.²⁵ A cynic might say that it was designed to subtly fend off our criticism of policy inaction.

Perhaps more important was an actual change in July. Executive Order 13010 on critical infrastructure protection prescribes responsibilities for protecting critical national information systems and networks, thereby responding directly to one of our recommendations. The Administration nonetheless failed to act with respect to the need to focus on the promotion of computer and communications security in the private sector. The reason is probably that they are still more worried about too much use of cryptography from the standpoint of law enforce-

ment interests than about too little use of it from the standpoint of preventing crime and protecting national security interests through protecting our technology and business firms.

The big change came on October 1, when the Vice President announced that the Administration was indeed ready to allow the ready export of 56-bit DES.²⁶ Indeed, it was ready to do so without key escrow. If it were not for the fine print, one could be tempted to call this response a ringing endorsement of our most far-reaching recommendations.²⁷

The most that can be said is that the DES proposal represents a step in the right direction. The right to export DES is to be limited to two years and is subject to prior approval of a plan by the vendor to build into its product an escrowed encryption solution. Moreover, within those two years there are to be milestones to assure steady progress toward the goal of having key escrow in place for each product at the end of the two years.

It would require too much clairvoyance and inside knowledge to know whether this approach will work. Certainly the attempt to use the right to export as leverage on the industry to support key escrow is at odds with the philosophy of our report as I have outlined it. On the other hand, the Administration had extensive private discussions with the relevant companies before making the October announcement. And several companies, notably IBM and Hewlett-Packard, have made announcements purporting to resolve some of the problems.²⁸ Nonetheless, press reports also indicate considerable, and growing, software industry dissatisfaction with the Administration's apparent interpretation of its own October initiative.²⁹

²⁶ The White House, Statement of the Vice President (Oct. 1, 1996).

²⁷ Administration of Export Controls on Encryption Products, Exec. Order 13026 (Nov. 15, 1996).

²⁸ The key escrow aspect of the Hewlett-Packard approach is based on Trusted Information System's RecoverKey technology. See Trusted Information System's Press Release, TIS's Key Recovery Technology Chosen by Hewlett-Packard for New Initiative (Nov. 18, 1996), available from the TIS Internet site.

²⁹ John Markoff, "A Compromise on Encryption Exports Seems to Unravel," *New York Times* C1 (Dec. 6, 1996); Bart Ziegler, "Group Blasts U.S. for Modifying Encryption Pact," *Wall Street Journal* B9 (Dec. 6, 1996). See also letter from Business Software Alliance to Messrs. McConnell and Appel, dated Nov. 8, 1996 (available from BSA).

²⁵ Executive Office of the President, Draft Paper, Enabling Principles, Commerce, Security and Public Safety in the Global Information Infrastructure (May 20, 1996).

It may be that the Administration's approach will work and that we will have in place a secure and efficient key escrow system two years from now. If so, bravo!

Still, problems lie ahead. Will other countries, particularly those suspicious of the United States, be willing to allow the import of encryption with the keys stored in the United States? Will foreign companies be willing to buy under those circumstances? Perhaps these difficulties can be resolved by government-to-government agreements. Our committee spent a good deal of time trying to come up with a workable international system that would avoid these and other difficulties but had to give up.³⁰

Perhaps we will not see a workable key escrow system in place two years from now. Will the Administration then be able to cut back on DES export? A cynic might think that the effort to use the right to export in this way is likely to fail, but the value of the approach, from the standpoint of the Administration, may prove to be that it will provide a graceful way out of a defective, unimplementable concept of key escrow.

Perhaps we will need another NRC study two years for now. After all, we emphasized that technology was changing so fast that our recommendations could only be considered part of a transition to an unforeseeable future.

³⁰ Much of the committee analysis is nonetheless to be found in NRC Report 243-244, 256-257 and Appendix G, at 430.

OCCASIONAL PAPERS FROM
THE LAW SCHOOL
THE UNIVERSITY OF CHICAGO
1111 EAST 60TH STREET
CHICAGO, ILLINOIS 60637

- No.1. "A Comment on Separation of Power"
Philip B. Kurland, November 1, 1971.
- No. 2. "The Shortage of Natural Gas"
Edmund W. Kitch, February 1, 1972.
- No. 3. "The Prosaic Sources of Prison Violence"
Hans W. Mattick, March 15, 1972.
- No. 4. "Conflicts of Interest in Corporate Law Practice"
Stanley A. Kaplan, January 10, 1973.
- No. 5. "Six Man Juries, Majority Verdicts—What
Difference Do They Make?"
Hans Zeisel, March 15, 1973.
- No. 6. "On Emergency Powers of the President:
Every Inch a King?"
Gerhard Casper, May 31, 1973.
- No. 7. "The Anatomy of Justice in Taxation"
Walter J. Blum and Harry Kalven Jr.,
October 1, 1973.
- No. 8. "An Approach to Law"
Edward H. Levi, October 15, 1974.
- No. 9. "The New Consumerism and the Law School"
Walter J. Blum, February 15, 1975.
- No. 10. "Congress and the Courts"
Carl McGowan, April 17, 1975.
- No. 11. "The Uneasy Case for Progressive Taxation
in 1976"
Walter J. Blum, November 19, 1976.
- No. 12. "Making the Punishment Fit the Crime:
A Consumers' Guide to Sentencing Reform"
Franklin E. Zimring, January 24, 1977.
- No. 13. "Talk to Entering Students"
James B. White, August 15, 1977.
- No. 14. "The Death Penalty and the Insanity Defense"
Hans Zeisel, April 15, 1978.
- No. 15. "Group Defamation"
Geoffrey R. Stone, August 10, 1978.
- No. 16. "The University Law School and Practical
Education"
Carl McGowan, December 20, 1978.
- No. 17. "The Sovereignty of the Courts"
Edward H. Levi, July 15, 1981.
- No. 18. "The Brothel Boy"
Norval Morris, March 15, 1982.
- No. 19. "The Economists and the Problem of Monopoly"
George J. Stigler, July 1, 1983.
- No. 20. "The Future of Gold"
Kenneth W. Dam, July 15, 1984.
- No. 21. "The Limits of Antitrust"
Frank H. Easterbrook, April 15, 1985.
- No. 22. "Constitutionalism"
Gerhard Casper, April 6, 1987.
- No. 23. "Reconsidering Miranda"
Stephen J. Schulhofer, December 15, 1987.
- No. 24. "Blackmail"
Ronald H. Coase, November 14, 1988.

- No. 25. "The Twentieth-Century Revolution in Family Wealth Transmission"
John H. Langbein, December 8, 1989.
- No. 26. "The State of the Modern Presidency: Can It Meet Our Expectations?"
Stuart E. Eizenstat, March 10, 1990.
- No. 27. "Flag Burning and the Constitution"
Geoffrey R. Stone, May 1, 1990.
- No. 28. "The Institutional Structure of Production"
Ronald H. Coase, May 15, 1992.
- No. 29. "The Bill of Rights: A Century of Progress"
John Paul Stevens, December 1, 1992.
- No. 30. "Remembering 'TM'"
Elena Kagan and Cass R. Sunstein, June 8, 1993.
- No. 31. "Organ Transplantation: Or, Altruism Run Amuck"
Richard A. Epstein, December 1, 1993.
- No. 32. "The Constitution in Congress: The First Congress, 1789-1791"
David P. Currie, June 15, 1994.
- No. 33. "Law, Diplomacy, and Force: North Korea and the Bomb"
Kenneth W. Dam, December 15, 1994.
- No. 34. "Remembering Nuremberg"
Bernard D. Meltzer, December 20, 1995.
- No. 35. "Racial Quotas and the Jury"
Albert W. Alschuler, February 20, 1996.
- No. 36. "The Restructuring of Corporate America"
Daniel R. Fischel, June 20, 1996.
- No. 37. "Constitutional Myth-Making: Lessons from the *Dred Scott* Case"
Cass R. Sunstein, August 26, 1996.
- No. 38. "The Role of Private Groups in Public Policy: Cryptography and the National Research Council"
Kenneth W. Dam, January 15, 1997.