INTERNATIONAL SYMPOSIUM ON THE PUBLIC VOICE AND THE DEVELOPMENT OF INTERNATIONAL CRYPTOGRAPHY POLICY

CENTRE DES CONFÉRENCES INTERNATIONALS

PARIS, FRANCE

25 SEPTEMBER 1996

OECD CRYPTOGRAPHY GUIDELINES IN CONTEXT

The Hon Justice Michael Kirby AC CMG

INTERNATIONAL SYMPOSIUM ON THE PUBLIC VOICE AND THE DEVELOPMENT OF INTERNATIONAL CRYPTOGRAPHY POLICY

CENTRE DES CONFÉRENCES INTERNATIONALS

PARIS, FRANCE

25 SEPTEMBER 1996

OECD CRYPTOGRAPHY GUIDELINES IN CONTEXT

The Hon Justice Michael Kirby AC CMG*

A NOSTALGIC LOOK BACK

We are in Paris once again. If I close my eyes nearly twenty years of my life roll way. I am once again chairing the OECD Expert Group on Transborder Data Flows and the Protection of Privacy.

---

* President of the International Commission of Jurists. One-time Chairman of the OECD Expert Group on Transborder Data Flows and the Protection of Privacy and on Security of Information Systems. Formerly Commissioner of the WHO Global Commission on AIDS and Special Representative of the Secretary-General of the United Nations. Justice of the High Court of Australia. Personal views.

The First Expert Group

It is important to view the OECD work on cryptography policy in the context of its institutional lineage. It is a project which follows directly upon the recommendation of the Council of the OECD of 23 September 1980[1] commending to member

---

1 C(80) 58/FINAL.

governments the Guidelines developed by the first Expert Group. It also follows the recommendation of the Council of the OECD concerning the Guidelines for the Security of Information Systems, adopted on 26 November 1992[2]. But more fundamentally, the new Guidelines will, in due course, be proposed to the Council of the OECD, a body established by its Convention[3] with the economic focus that its title suggests but agreed between nations which have certain precious things in common. These are a commitment to the rule of law; an acceptance of the democratic system of government; and a respect for fundamental human rights.

These features of the OECD are reflected in the Guidelines recently published by the Organisation in its Development Cooperation Guidelines Series. The Guidelines are concerned with *Participatory Development and Good Governance*[4]. They relate to the integral role which good governance plays in economic development. They represent more than pious homilies addressed to the developing countries which seek the assistance of OECD Member States. In a very real sense, they

---

2 C(92) 188/FINAL.

3 Convention on the Organisation for Economic Cooperation and Development of 4 December 1960.

4 OECD, 1995, Paris.

represent the statement of the kind of ties which the OECD States share in common and which bind them together.

Amongst the important statements in the Guidelines are the following:

> "33. A predictable legal environment, with an objective, reliable and independent judiciary, is an essential fact for democratisation, good governance and human rights. The protection of human rights requires a legal system capable of fulfilling certain fundamental requirements: government should exercise its powers in accordance with the law; there should be an independent court system; the system should have full constitutional rights to investigate and supervise the exercise of executive and administrative powers[5].
>
> 68. DAC Members recognise the role of non-governmental human rights groups in promoting human rights. They are a source of information on human rights situations and a constituency for human rights vis-à-vis governments and public opinion. In developing countries, human rights NGOs are often 'first-line-of-defence' organisations whose members in some cases take considerable risks. DAC Members recognise their independence and the need to promote human rights NGOs and other defenders of human rights[6].
>
> 70. Several aspects of human rights are particularly important for development. These include:
>
> - The Vienna Declaration states that democracy, development and respect for human rights and

---

5 *Ibid,* 14.

6 *Ibid,* 23-24.

> fundamental freedoms are inter-dependent and mutually reinforcing.
>
> - Respect for human rights gives scope to the creative energy of people and prevents scarce resources being used by a repressive apparatus.
>
> - Human rights and fundamental freedoms such as freedom of expression, assembly and association empower people in their struggle to improve their living conditions and make it possible for civil society to criticise and redress unjust or inefficient State policies. A free press will greatly facilitate these processes[7]."

What is sauce for the goose is sauce for the gander. This instruction to developing countries is properly turned back to the OECD Member States themselves. In the development of cryptography policy, it is essential that the rule of law, respect for human rights and respect for the rights of NGOs should be fully protected.

In 1960 when the OECD was established, in the midst of the Cold War, the reference to these special features of OECD countries did not need to be over-stated. They were just assumed by everyone. They were the things that made the OECD a unique and special place: quite different from other international bodies. This was not only just a club of the developed and richer countries of the world, exchanging

---

7 *Ibid,* 24-25.

information vital for their continued economic success. It was also an organisation whose members accepted certain governmental norms and principles. It is important to remember these features of the OECD at the outset for they provide the *milieu* within which the cryptography policy guidelines must be fashioned for presentation to the Council of the OECD, still representing the governments that share these common features.

It is worth recalling to mind, just for a moment, the remarkable and talented groups of people who made up the two earlier Expert Groups. They included some of the most intelligent people I have ever worked with. Many of them have gone on to distinguished national and international service. Mr Louis Joinet became an adviser to the President of the French Republic and is one of the Special Rapporteurs for Human Rights of the United Nations. Mr Hans Corell of Sweden went on to become the General Legal Counsel to the United Nations. The same high talent was seen in the second group. Both groups were well served by the OECD Secretariat, led by Mr Hans Peter Gassman, ably supported by Professor Pieter Seipel and Mrs Deborah Hurley. It is not an exercise in nostalgia to say this. It is a reminder of the fact that the high success of the earlier Guidelines derived from work of people of considerable talent, a strong sense of independence and a good understanding of the context of international human rights law within which they were drafting their Guidelines.

I do not pretend that the battles over human rights issues did not sometimes have an economic dimension. Thus, in the first Expert Group, the commitment of the United States to free flow of information in TBDF was said to draw strength not only from that country's political and legal culture but also from its then dominance of information technology. On the other hand, the European countries' commitment to privacy protection drew on the experience of those countries in the misuse of information system during the War. But it was also said to take strength from a desire in Europe to promote a local information industry. However that may be, the experts were able to reach the necessary compromises. The Guidelines were agreed. They were recommended to, and adopted by, the Council. And all this was done in the usual way of the OECD. Patient consensus building rather than impatient demand for action is the way that the OECD operates. A measure of the success of the Guidelines on Privacy, sixteen years later, is the extent to which they have been adopted, virtually unaltered, in the domestic law of several member countries of the OECD, including my own[8]. The Guidelines for the Security of Information Systems have also proved influential in many countries, providing the impetus to the consideration of local laws and policies.

---

8 *Privacy Act* 1988 (Aust).

It is self-evident that this history of the development of Guidelines, in the context of international information policy, is a most precious resource of the OECD. It is respected and valued in the member States and beyond. It will be most important that nothing be done in the preparation of the Cryptography Policy Guidelines which diminishes the high reputation which the OECD Expert Groups enjoy in this field both for their product and for their methodology.

This needs to be said because, in the field of cryptography, as in the earlier areas of privacy and security, a failure of the OECD's efforts, or attempts of individual member States to "go it alone" are likely to prove ineffective, inefficient, such as will impair international trade and retard the development of the Global Information Infrastructure and the Global Information Society. These goals are important not only for the future economic well-being of OECD Member States but of the whole world. Moreover, they are part of the definition of the future of our world in which human beings everywhere will flourish and enjoy the stable, ordered, democratic and rights-respecting environment which the current members of the OECD generally enjoy. It is inevitable that the Council of the OECD will want to hand that legacy on to future generations, enhanced and not diminished by advances in information technology. All of this may be accepted. The question presented by developments of information technology relevant to cryptography is whether these

have changed the "playing field" such that new large powers must be afforded to the state to monitor and intrude into information systems, including those which have been encrypted to protect integrity, confidentiality, privacy and other qualities of information.

I do not pretend to a detailed expertise in the issues which the cryptography guidelines will present for debate. At this stage the draft is restricted. But in the twenty years since I first laboured over OECD Guidelines, I have had much experience in several international and national bodies relevant to human rights. Back in 1978, the OECD "house" felt a little uncomfortable in tackling the issue of privacy, so manifestly an issue of human rights. It was not the usual fare of the economists, technologists and government officials who walked the corridors of the OECD. But since then, stimulated in part by the achievements of the earlier experts groups and by a realisation of the very things which bind the OECD together, the issues of human rights have been assuming a higher agenda in the OECD, and rightly so. Not only do human rights have strong economic implications. They are the cement which binds together the member States of the OECD and provides the rationale for the existence of the Organisation: by economic cooperation and development to strengthen the social and individual environment within which the citizens of the OECD countries live and work. After all, economics has no point in itself, save as it serves and enriches the lives of individuals.

LESSONS FROM A DIFFERENT WORLD

Now let me take you into a different world. It is the world that has brought me from Australia to Europe on this visit. Recently, I have moved out of the field of information policy to other pressing concerns of the international community. One of them is the Human Genome Project - the greatest international scientific cooperative project in history[9]. But another is HIV/AIDS. Each of these projects - the genome and AIDS - represents a development that is of enormous economic potential, including for the member States of the OECD. Each poses important challenges to human rights. Each must develop within the context of international human rights law. Each presents highly controversial problems which are extremely difficult for democratic societies to solve without the help of informed experts and international cooperation.

The immediate reason for my visit to Europe is a meeting at the Palais des Nations in Geneva for a consultation on human rights issues of HIV/AIDS summoned by the High Commissioner

---

9 The author is now a member of the Ethics Committee of the Human Genome Organisation and of the International Bioethics Committee of UNESCO.

of Human Rights and UNAIDS - the joint programme on AIDS established by the Secretary-General of the United Nations. I was elected chairman. I express my gratitude to them publicly for releasing me from a morning session of their consultation so that I could come to this symposium in Paris. They agreed that the issue you are addressing is also of great importance to the international community and to human rights. That is why they let me come.

Permit me to draw upon my work of the last decade in policy development on HIV/AIDS, including in the WHO Global Commission on AIDS, to extract a number of lessons which, I believe, provide the framework within which cryptography policy guidelines should be developed by the OECD Expert Group. Let me suggest that there are ten commandments:

1. ***Accurate technical data:*** The first rule I learned in the provision of advice on global strategies to meet the challenge of HIV/AIDS was to rest all policies and laws upon sound scientific data. Not hunch or guesswork, prejudice or good theories. But a sound understanding of the virus, its modes of transmission and its real challenge to the international community. It is the same with cryptography. The technology is moving most rapidly: from Clipper to Capstone. From Fisher Watchdog, Entrust, Stoplock, Secure through Key Escrow, Weak Encryption, Link Encryption and Strong Encryption. The starting point

the governmental programmes of those countries, such as my own, which have actually made an impact on containing the epidemic. I think that this is important in the field of cryptography as well. I applaud the involvement by the OECD of trade, industry, telecom, law enforcement, national security, private sector and data protection agencies in the work of the Expert Group. But it will also be vital, if the programme is to be a success in practice, closely to involve those bodies that speak for values which may sometimes be in competition. One of the real successes of the international and national work against HIV/AIDS has been the involvement of non-governmental organisations who speak up for the infected, their families and carers. It is equally vital in the work of the Expert Group on Cryptography that its product should be exposed before completion to the critical attention of civil society organisations which speak, for example, for privacy, for individual rights and for the containment of the power of surveillance by the organs of the State. If it is not done by the Expert Group in Paris one thing is sure. The Guidelines, when returned to the member States with the recommendation of the Council of the OECD, will fall into the net of community debate about the privacy and other concerns. If real action on the OECD Guidelines is sought, it is vital that strong voices for the relevant human rights should be expressed at the OECD table. This was done in the earlier Expert Groups, often by the experts

themselves and sometimes by invited observers. There would be a danger if the issues of cryptography, for example, were turned over to the viewpoint of law enforcement and national security representatives (however important) to the effective exclusion of advocates of privacy and democratic rights.

5. ***Language and symbols:*** One thing has been learned in the struggle against HIV/AIDS and that is the importance of language and of symbols. Especially against the background of past epidemics, and the highly ineffective but oppressive responses of nations and of the international community, there is often alarm at the dangers to individual rights which can actually be counter-productive in tackling the problem. So too in cryptography. It is important that there should be no under-estimation of the significance of the symbols which will be sent out by the Guidelines to the various audiences which will be scrutinising them in the free societies of the OECD. Thus, to delete references to privacy, or to regard them as adequately covered by the historical allusion to the previous Guidelines, would not be missed by those who champion privacy concerns. In the business of international guidelines, language and symbols assume a rare importance for they are the signals to action in the governments to which the guidelines will be addressed.

6. ***Alarm in proportion:*** It is important that the Guidelines should be based not only on sound scientific understanding of the nature of cryptography and what is and will be available. But also on a clear understanding of the social problems which are said to give rise to the need in government to break the encryption and invade it. Encryption is not the only protection for privacy; but it is one protection. The demands for the right to governmental intrusion into private messages and commercial secrets are usually expressed in extremely general language:

> "These cases involve child pornography, customs violations, drugs, espionage, embezzlement, murder, obstruction of justice, tax protesters and terrorism. At the International Cryptography Institute held in Washington in September 1995, FBI Director Louis Freeh reported that encryption had been encountered in a terrorism investigation in the Philippines involving the alleged plot to assassinate Pope John Paul II and bomb a US airline[11]".

These suggestions paint opponents to the enhancement of government power into a corner as those favouring child pornography (at the top of the list), terrorism and the assassination of the Pope. Who could favour such things? But the lesson of the response in democratic societies to terrorism has been the importance of resiting extreme

---

11 Denning, above n 6, at 34.

authoritarian measures in the attempt to combat it. When authoritarianism prevails, the terrorists actually win. The lesson from HIV/AIDS is that alarmist talk must be viewed with real suspicion and subjected to cold-eyed scrutiny to measure the real scope of the problem that is said to require extreme measures.

7. ***Tripartite test:*** Another lesson from HIV/AIDS is that the policies and strategies must be developed in a context of international law. This requires that they should respect fundamental human rights, such as the right not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence[12]. With the advent of the HIV/AIDS epidemic public health officials demanded complete exemption from human rights restraints. However, it is now generally understood that those restraints must be kept in place. Any derogation from fundamental rights must be subject to three limitations:

(i) that they are authorised by law not secret and not arbitrary;

---

12 *International Covenant on Civil and Political Rights,* Article 17.

(ii) that they are confined to the minimum that is absolutely necessary for the protection of society; and

(iii) that the competing objective is one which is compatible with the requirements, institutions and assumptions of a democratic society.

I suggest that the same three limitations apply to each and every demand by national security and law enforcement agencies for a power to monitor information, including that subject to strong encryption. No individual or agency is above the law in OECD countries. Nor should they be.

8. ***Ongoing action:*** Another lesson is that the target of policy and law constantly shifts. The virus mutates. New areas of the globe with different problems are attacked. So it will be with cryptography. The technology, the national interests and the skills and capacities of individuals will change rapidly. Already in significant respects the 1980 Guidelines on Privacy have been overtaken by new technological capacities of information systems. There should be a healthy modesty in the views of the Expert Group as to what they can achieve. They need to recognise that the task in which they are engaged in is an ongoing one, although it presents immediate and urgent dilemmas.

9. ***Government role:*** There is also an urgent need to capture the attention of governments at the highest level. This is so in HIV and it is so in cryptography. Alas, in the former, governments tend to run away from responsibility. The problem in cryptography may be the exact opposite. The voices of national security and law enforcement agencies will generally be close to the ear of government. It is important that there be voices of equal strength to speak for human rights, the rule of law and protecting the privacy of citizens from the technologically enhanced capacity of the State to monitor their communications. In Australia, citizens with a concept of the rule of law have been shocked by the recent revelations of corruption and manipulation involving the nation's largest police force (the New South Wales Police Service). Last week a further inquiry began into the Federal Police because of allegations of corruption. I am sure that my country is not alone in this danger. Where trade secrets, governmental data and vulnerable systems are at stake it is imperative that those who claim the key to the kingdom of encryption should themselves be subject to constant and fearless scrutiny against the misuse of such large power.

10. ***Action for effectiveness:*** In the battle against HIV/AIDS there is a role for governments and their agencies to take action. But in a democratic civil society most of the

effective action will take place amongst individuals and community groups. The task is to define the limited role of government action and then to keep its agencies within that role. They should be subjected to stern legal discipline and constant scrutiny to ensure that the agencies remain our servants, accountable to the elected representatives of the people. It is a healthy democratic principle for citizens of democratic countries to remain highly sceptical of alarmist protectors. The history of this century has been one of the misuse of power. Technology now enhances the power of intrusion. In the name of human rights, including privacy, it is important that the powers of intrusion, including official intrusion, be kept in strict check. I suggest that such checks can be fashioned by reference to my commandments, and doubtless others.

CONCLUSIONS

I offer my respects to those who have the privilege to participate in the OECD Expert Group which follows those I was honoured to chair. I know enough of the problem of cryptography to realise that it is not easy of solution. The issue is not, as I think, one of "balancing" the legitimate aims of law enforcement and national security (on the one hand) and protection of privacy and other human rights (on the other). Each of these objectives has a legitimate claim on governmental policy and action. However, the claims of national security and

law enforcement agencies have to be attained within a context of constitutionalism, the rule of law and respect for, and effective protection of human rights. This was recognised by the earlier Expert Groups. It is, I believe a reason for the success of the Guidelines which they produced. Those Guidelines were themselves the product of free citizens, working together in the harmonious community of the OECD. It is imperative today to retain the momentum and the approach which the earlier Expert Groups embraced. This is not only important for the reputation of the members of the present group or of the OECD. It is important for the good government and happiness of the citizens of the member countries.

Sometimes it is useful to see one's problems through the prism of a different experience. That is why I have been brought from another world (well actually Geneva) to offer these few remarks. For the affection for the OECD, forgive an old participant. For the recognition of the limited but legitimate role for national security and law enforcement, I plead a judge's understanding of the exceptional cases, under legal warrant, where this may be justified and even imperative. But for the demand for effective respect of human rights, and especially individual privacy, I make no apology. Such rights represent the ultimate common denominator of the OECD. They should find reflection in the new Guidelines as they did in those that went before. The Expert Group will want nothing less. Nothing less will do.