

## Chapter 6<sup>1/2</sup>. Outlawing cryptography

*If cryptography is outlawed, only outlaws will have cryptography.*  
(Phil Zimmerman)

When a state has a problem, its most natural reaction is to outlaw its cause. For instance, if a particular society considers it wrong to kill people, it establishes a general ban on murder. If a government thinks that it is wrong to kill, but that it may be useful for itself, it creates an exception for itself only (the death penalty). Or if a society considers it good to kill someone if it is the best option given the circumstances, it may allow a generic exception under strict conditions (euthanasia, self-defense). Or even, a society may consider it appropriate for individuals to kill in specific cases (vendetta, suttee).

Prohibiting activities which have only – or mainly – negative implications is easy. The few legitimate exceptions may be addressed by granting generic licenses or individual licenses. With actions that have good sides as well as bad sides, it becomes more difficult to create a general ban. And if an activity is generally good, but has a few bad effects as well, a general prohibition with licenses for the legitimate uses is twisting round exception and rule.

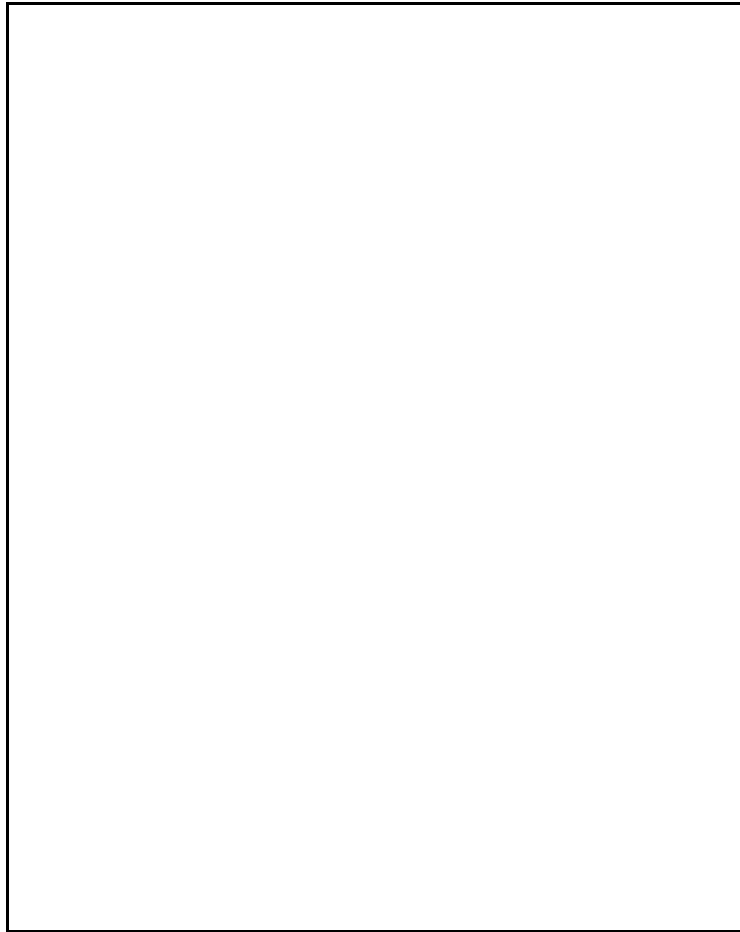
Prohibiting is only an option if the negative implications of the contentious issue significantly outweigh the positive sides. With cryptography, that is not the case: it has a crucial role to play in the information society, and the negative effects of criminal (ab)use of crypto in no way outweigh its benefits. Outlawing cryptography (with licenses for certain (government-friendly) crypto types or individuals who might need it) is simply not a real option, and that is why this chapter is not a real chapter.

However, the idea of a crypto ban has actually occurred to some governments (even to the Dutch government, which one would have expected to be more sensible), and mandatory government-accessible crypto is still advocated in several government circles. It therefore seems wise to go at least briefly into the main arguments against a ban on cryptography.

If a ban on cryptography is to aid law-enforcement, the aim will be to make sure that people do not use encryption, or that they use only cryptography that provides for law-enforcement access (mainly through access to keys, which I call ‘LEAK’ – Law-Enforcement Access to Keys, see Chapter 7). The ban may be all-encompassing, or it may allow certain types of cryptography to be used, for instance, weak cryptography or LEAK-enabled crypto (mandatory LEAK). It may target the manufacture, trade, import, or use of non-LEAK cryptography. It could also allow non-LEAK crypto use for specific applications (such as banking) or for users that will not hamper law-enforcement (such as the government itself).

But whatever the kind and scope of the ban or mandatory LEAK legislation, if its aim is to ensure that the police can continue to understand wiretaps and computer files obtained

through a search, one must assess how the ban helps law enforcement (6½.1), and how it affects the security and privacy of citizens and the economic implications for society at large (6½.2).



*Figure 6½.1. Page from an FBI presentation on encryption policy, discussing the need for a prohibition of non-LEAK cryptography. Obtained by the Electronic Privacy Information Center. [source: EPIC]*

### **6½.1. A crypto ban does not help the police**

A crypto ban is not enforceable. First of all, strong, non-leak cryptography will continue to be easily available to criminals, especially (but not only) to those with some resources. After all, strong cryptography abounds nowadays, and is still continuing to spread. In practice, a government can never make sure that all the present crypto software and hardware are

destroyed. Those criminals who do not yet have a crypto program, may easily avail themselves of an old copy – banned cryptography would simply become an interesting black market. Moreover, simple yet effective crypto algorithms are described in handbooks, and they are fairly easy to implement.<sup>1</sup> Easiest of all, you can download good cryptography from the Internet. Even if one considers it realistic (which it is not) that all ‘sensible’ countries would outlaw cryptography, ‘crypto havens’ would emerge, and crypto-anarchist communities would, out of principle, love to cater to crooks and criminals through the Internet. A crypto ban will simply not be able to deny easy access to strong, non-LEAK crypto.

A second argument why a crypto ban is not enforceable, is that it is hard to monitor. Obviously, the police cannot check all computers and diskettes for the presence of banned cryptography. Monitoring encrypted communications is likewise a considerable challenge. Where monitoring public roads for speed-limit offenses is hard to keep up on a reasonable scale, monitoring electronic highways for crypto-use compliance on any scale will be even harder. The amount of traffic is enormous, and the monitoring would have to be automated in some way. Now this is problematic, given the diversity of formats and programs used – it is not easy to distinguish off-hand and automatically between encrypted data and other collections of bits and bytes (see sidebar on next page). The only way a knowbot (a robotic piece of software which automatically performs a pseudo-intelligent task) could distinguish between ‘legal’ data (encrypted or not) and illegally encrypted data, is to monitor headers or pre-fixed formats.<sup>2</sup> Such traffic monitoring would only be practical if the bulk of communications traffic used distinguishable headers or formats, and this is quite unlikely to achieve in the current international situation. Even then, the ever-resourceful crypto-anarchic community would develop programs which use illegal crypto while producing acceptable headers or formats that would fool the knowbot monitors; such programs would easily find their way to cryptocriminals. The police will lose the monitor race from the beginning.

Apart from general automated enforcement, a case-by-case monitoring would also often be fruitless. There are well-known ways to escape it. Steganography (see 3.1.8) can hide ciphertext in seemingly innocent data. This is not practical in all cases, but a crypto ban could spur opponents (and there are many opponents in the cryptographic community) to devote their efforts to develop more sophisticated and practical systems of steganography. Moreover, a crypto ban would push criminals to start using steganography, even when they would not otherwise consider the effort worth while. Although, in principle, the police may often be able to unmask steganography, this is resource-consuming and not practical on a large scale. Moreover, apart from steganography, there is a much easier way to escape enforcement: use superencryption. Cryptocriminals will first use an illegal crypto system (which, as noted, is easily accessible) and then encrypt the ciphertext with a legal crypto system.

- 
- 1 “Talent for hire is easy to obtain. A criminal party could easily hire a knowledgeable [sic] person to develop needed software. For example, an out-of-work or underemployed scientist or mathematician from the former Soviet Union would find a retainer fee of \$500 per month to be a king’s ransom.” [NRC, 269]
  - 2 For a possible way of monitoring a LEAK-compliant crypto infrastructure, see [Verheul 97a]. With such a system, there are still easy ways to comply with the required format while not giving law enforcement access to keys (cf. Chapter 7).



#### Mandatory LEAK and constitutional rights

Mandatory LEAK systems are often claimed to infringe constitutional rights disproportionately. Especially within the cypherpunk community, one often hears the argument that people have an (intrinsic) right to encryption. The argument often centers around the freedom of speech: people argue they have the right to say anything they want in any way they like. The argument fails, in my opinion, to recognize that the freedom of speech primarily addresses speech content, not the medium used for conveying the speech. Newspapers can refuse letters to the editor out of space considerations, and people hardly argue this infringes their right to freedom of speech. If you cannot publish your opinion in the *New York Times*, you spread a leaflet, target the radio, or publish a newspaper yourself. Freedom of speech only addresses the medium of speech in that everyone must have an *adequate* means of expression (not *any* means to one's choice). Prohibiting newspapers altogether may well be compatible with freedom of speech, if there remain sufficient other means of expressing one's opinion to a similar effect, and if it is a proportional measure.

I would argue that likewise, there is no fundamental 'right to encryption' through freedom of speech. If you cannot use the particular encryption system you want for communicating your views, use another medium – a crypto system that *is* allowed, communication in person, or, why not, a Kwakiutl courier. Also, remark that freedom of speech safeguards the possibility of making your opinion *public*, whereas encryption is used to keep your opinion *private*. Even if LEAK schemes were built-in in a significant portion of people's communications media (e.g., in web browsers and operating systems), and people would thus be more or less obliged to use them, this would not infringe upon their freedom of speech: they can still express their opinion – the fact that law-enforcement agencies could access this opinion does not alter this. Therefore, I do not think that mandatory crypto systems in general infringe upon the freedom of speech.

The US First Amendment may be more extensive than the Dutch understanding of the freedom of speech, but it can well be argued that mandatory LEAK does not infringe the First Amendment either, as Robert Litt, principal associate deputy attorney general, has aptly done in Congress [Litt]. His argument only falters with two possible infringements. First, mandatory LEAK may unduly restrict the ability of cryptographers to exchange crypto source codes (cf. the *Bernstein* decision). This, to me, seems a minor infringement one might consider proportional, given the major concerns at stake. However, the other potential infringement Litt does not adequately refute: the potential chilling effect of mandatory LEAK on free speech. People may feel restricted to communicate over a LEAK infrastructure. Litt rejects this with the argument that LEAK does nothing more than preserve the current capability of wiretapping, which, the court has decided, does not 'chill' free speech. There may, however, be good arguments to see the chilling effect of a LEAK infrastructure as larger than that of a wiretap-enabled telephone network. Communications patterns are changing with the advent of the information society, and larger parts of private life are taking place online. Therefore, the fact that governments could access these extended patterns of communications might ultimately have a chilling effect on free speech. This is not an argument that people in the Netherlands would consider valid, but in the US, it may hold more strength.

The 'right to encryption' has more to do with the right to confidential communication. This constitutional right is part of people's right to a private sphere (e.g., art. 17 ICCPR, art. 12 UDHR). The right to confidential communications implies that people must be able to choose adequate protection measures for safeguarding confidentiality. Thus, if governments consider making LEAK schemes mandatory, they have to ensure the system is secure against unlawful eavesdropping. Moreover, inasmuch as the LEAK system allows law-enforcement agencies a wider access to people's communications than they currently have, this ability must be established by formal law after a careful balance of the concerns involved. For the moment, as long as governments cannot guarantee the security of LEAK systems [cf. Abelson 97], one can argue they cannot make them mandatory. In the US, the Fourth Amendment protects reasonable expectations of privacy by prohibiting unreasonable searches. A LEAK infrastructure need not harm this expectation, if proper conditions for law-enforcement access are enacted. [Litt]

One could also suggest that obliging people to escrow their private keys infringes the privilege against self-incrimination. After all, you oblige people to give the police the means to gather evidence against them. For several reasons, the argument does not hold. First, the right to non-self-incrimination pertains to suspects, whereas a mandatory LEAK system is a general measure targeting citizens at large; people depositing their keys do not do so in a capacity of criminal suspect. Moreover, the concern protected by the privilege against self-incrimination is that the truth be found in criminal proceedings (see 8.5). Now, requiring people to use means that enable law-enforcement agencies to gather evidence does not threaten the fact-finding process, as people are not forced to give evidence itself. After all, people may refrain from using the LEAK system; they are not in any way obliged to use it for communicating incriminating evidence. There are plenty of parallels, for instance in the tax-law requirement of keeping verifiable books: this also is a requirement that creates the possibility for law enforcement to gather evidence, while it does not concretely push people to hand over incriminating evidence. The same arguments imply that mandatory LEAK does not infringe the Fifth Amendment. (See Chapter 8 for an analysis of the privilege in relation to demanding decryption.)

Knowbots and human monitors will regard the message as legal, until they decrypt it and find it contains another layer of encryption underneath (or is it an exotic image format, or perhaps Chinese big-5?). Of course, the monitors will seldom decrypt ‘legal’ messages, and the bulk of the ‘illegal’ messages will go unnoticed.

In conclusion, a crypto ban is unenforceable, and even if it were enforceable – in the sense that prohibited crypto use could be monitored – cryptocriminals could still easily escape notice. Illegal crypto use will only be noticed when it is too late: in a search, or after a wiretap. This suggests that it may be better (or rather, less bad) to restrict the ban to these situations: one could consider penalizing crypto use when this obstructs a criminal investigation (in particular, a search or a wiretap); the effects are the same for criminals facing investigation, but at least for law-abiding citizens, crypto use will be legal. There are objections to a prohibition of crypto use that obstructs investigation as well, but it may be an option to consider (see 8.7 – this non-chapter only deals with non-options).

### **6½.2. A crypto ban does hamper good guys**

Whereas most criminals will not be affected by a crypto ban, most law-abiding citizens will be. In the information society we are building, the vast majority of the public will be affected in two ways: individually, and collectively.

First, if cryptography is banned, would-be crypto users (and who would not be a crypto user in the information society?) face extensive security and privacy threats. This is also the case if they are allowed to use LEAKing cryptography. Any LEAK system weakens the security of cryptography (by definition, since an extra access feature for law enforcement creates new opportunities for attacks, such as bribery or counter-infiltration, and in practice, because the systems are more complex and thus may introduce new security leaks): the risks of LEAK cryptography are fundamental and significant [Abelson 97] (cf. Chapter 7).

A second possible effect of a ban of non-LEAK crypto on law-abiding citizens is that the balance between citizens and their government may turn significantly in favor of the government. Taking the pre-digital era as a reference point, the rise of information and communications technologies is affecting this balance in two ways. Most notably, cryptography allows citizens to effectively escape government’s scrutiny on a scale formerly impossible, which adds weight to the citizens’ level of power. On the other hand, ICT also allow new monitoring techniques (cf. Chapter 9), and the increasing registration of all levels of public life and of many levels of private life gives the government considerable powers over the citizen. These countering developments mean that the digital era does not necessarily alter the precarious balance between government and citizens. However, were non-LEAK cryptography to be banned, the balance inexorably moves towards the government. Whereas this is not an immediate threat in countries with good governance (in many countries featured in Amnesty International’s yearly report, one should consider this a threat), no government can ensure that powers will not be abused by future governments, as history has sadly shown so often. A LEAKing crypto infrastructure can be established with many checks and balances, but once the infrastructure is there, future abuse is easy and unavoidable once a

government turns crooked. Law-abiding crypto users could become future Winstons, desperately looking for a corner to escape Big Brother's persecution.

Finally, a crypto ban will also lead to a collective, economic backlash, since international trade will significantly be obstructed if companies cannot communicate or trade securely (cf. Chapter 3). If the ban is not enforced on an international level (comprising at least the G7, but preferably the OECD and ASEAN), companies in a crypto-banned country will have a hard time staying alive in the information society, since international traders will prefer secure transactions without foreign governments' access. Indeed, they may decide to move to another, more crypto friendly country, causing damage to the economy of the crypto-banning country. Now, worldwide consensus on a crypto ban is nowhere to be reached; the OECD principles do not rule out mandatory LEAK in explicit terms, but the wording is strong enough to suggest that an international crypto ban or mandatory LEAK is not an option.<sup>3</sup> Moreover, even apart from global competition, the costs for implementing a LEAK infrastructure are huge. All current software and hardware containing cryptography must be replaced, throwing away all investments in current information security. Also, the costs of maintaining a LEAK infrastructure are higher than those of maintaining a strong, non-LEAK infrastructure. Lastly, it seems undesirable that corporations who will comply with the crypto ban (and thus have more costs and less security) will be at an economic disadvantage with respect to businesses who use illegal strong cryptography (which, as noted, is hard to monitor and punish).

In short, a crypto ban has very serious consequences for law-abiding citizens. It poses a significant threat to privacy and information security, and it severely obstructs the development of the information society. It may also pave the way for future governments with less noble intentions to do away with privacy altogether. Finally, a national crypto ban will lead to a severe economic backlash.

### 6½.3. Conclusion

The conclusion of this non-chapter is short and simple. The gains of a crypto ban or of mandatory LEAK for law-enforcement are dubious at best, and more likely low to non-existent: it does not pose serious problems for criminals to use strong cryptography. The losses of a crypto ban for individuals, businesses, and the information society, on the other hand, are certain and large. There is no way to achieve any balance between these effects. It is, as Phil Zimmerman – ever the rhetorician – has suggested, like reverse chemotherapy: it kills the benign cells, while it leaves the malignant cells intact.

Banning cryptography or mandating LEAKing crypto systems is simply not an option. We had better move on to real chapters with real options.

---

3 “Government controls on cryptographic methods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible.” [OECD 97, principle 2]