CHALLENGES IN AGRICULTURAL AND RURAL DEVELOPMENT IN CENTRAL AND EASTERN EUROPE
ECONOMIC AND ENVIRONMENTAL STUDIES No. 6 OPOLE 2004

Joost PLATJE
Opole University (Poland)
Lesław TRZMIELEWSKI
The International School
for Logistics and Transport in Wrocław (Poland)

SUSTAINABILITY AND INFORMATION SAFETY

1. Introduction

In this article some aspects of information safety are discussed within the context of sustainable development. The importance of access to information is discussed in Section 2.1. However, as is argued in Section 2.2, there are cases when access to information should be limited because it can be a threat to sustainability. In such a case information should be protected. In Section 3.1 the security of sending electronic messages are discussed within the context of the costs and benefits of different types of protection. Some empirical research on decoding passwords for electronic messages is presented in Section 3.2. In Section 4 the main findings of this paper are summarised, and one of the conclusions is that information safety depends on the costs of breaking a code and an efficient institutional environment enforcing property rights on information.

2.1. Why is access to information necessary?

Environmental protection is according to art. 74 par. 2 of the Polish constitution an obligation of public authorities, while according to par. 3 everyone has the right to information on the state and protection of the environment [Konstytucja Rzeczpospolitej Polskiej, 1997, 42]. This implies that any citizen, regardless of nationality, has the right to this type of information. Following the Aarhus Convention, ratified by Poland in

February 2002 [Gubrynowicz, 2003], it is not necessary to give a reason why someone requests information. Thus, a lack of explanation in a request for information on the state of the environment and environmental protection cannot be a reason for public authorities to refuse the provision of information, although practice may be different.

Free flow of information is important for properly working markets and stimulating economic exchange, which may lead to an increase in the standard of living. As markets may create negative externalities in the form of pollution, excessive use of renewable and non-renewable resources, extinction of species, and so on, information on this is indispensable for internalising those externalities, in order to stimulate sustainable development. Sustainable development has been defined as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs."[1]

Proper access to information reduces the problem of asymmetric information [see Akerlof, 1970; Molho, 1997], where one party possesses more information on a subject that another party. For example, a factory may have more knowledge on the pollution it causes that citizens who are the victims of this pollution. Government agencies or non-governmental organisations, in general, have more opportunities to obtain information on this pollution than individual citizens. When, for example, the government possesses such information, citizens should have easy access to this information, in order to be able to reduce the damage. In this respect, participation of society and empowerment, in other words, the development of civil society, may be of great importance.

2.2. Why should access to information sometimes be limited?

Although access to environmental information is a right, there are exceptions. For example, according to the Council Directive 90/313/EWG from 7 June 1990, organs of state administration may (but do not have to) refuse access to information. The first case is when the information concerns international relations, national defence or public safety. In other words, access to information may be denied when it threatens political and economic stability. Another reason for denying access to information may occur when there are legal or disciplinary proceedings in progress, when it concerns personal data, or documents or data which are not yet complete. Free flow of information may in some cases be

[1] Brundtland Report, quoted in Rao [2000].

a threat to sustainable development and the protection of species. For this reason information about *e.g.* habitats of birds does not have to be disclosed. Furthermore, a request for information may be absurd or too generally formulated. In this case the transaction costs of finding and supplying information are too high, and resources would be wasted on this. Although this may be a good reason for state organs to refuse provision of information, this argument may be abused. How should one decide whether a request is too general or absurd? A request for certain information may seem absurd to a civil servant, but be highly relevant to a citizen, a scientist or representatives of business and non-governmental organisations (NGOs). For this reason, all stakeholders (state organs, citizens, business, NGOs and so on) should be involved in the establishment of rules in this field.

There are practical problems with access to information. The right of citizens to environmental information implies that a problem of asymmetric information exists. This means that not all information is public. Private information exists – one party possesses more information about the subject than another party. The transaction costs of obtaining information can be significant in terms of time and money. Poznanski [1996, xvii] argues that private information cannot become completely public "because of different experiences and perceptions of actors and the conditions under which information was accumulated by an actor." In other words, due to what Sen [1992] calls differing personal characteristics, communication of information may be hampered. As Poznanski goes on, the "best" conditions for communicating information are trust and repeated interaction. However, achieving such a situation is again connected with high transaction costs.

Thus, as Platje [2004] argues, there can be no 100% public information (abstracting from future information). The moment that there is no 100% public information, *e.g.* private property rights are established and enforced on certain information, leading to informational asymmetries, "market failures" come into being. However, a complete free flow of information can hamper economic development, for which reason intellectual property rights may be established. Business information and information on production processes may be protected in the case of patents. If all information became public immediately, the incentive to innovate or to introduce new management or distribution techniques, would be weaker. Thus, a perfect working market provides weak incentives for innovation, because information is publicly owned. However, it is not a public good in a dynamic world, because when someone uses the information regarding the new invention, it lowers the utility for someone else. The information can still be used, but becomes less useful. Or as

Heyne [1994, 183] puts it, "the most serious objection to any full disclosure requirement is that requiring people to reveal everything they know prior to any transaction would destroy much of the incentive to acquire costly but socially valuable information." (*e.g.* writers, inventors.) Thus, it can be argued that when an institution is created that would disclose information immediately, transaction costs are lower, but at the same time it provides disincentives to search for new information. In other words, private information stimulates economic activity to a certain extent.

Concluding, there are several reasons why access to information may be limited. In other words, access to information is required for achieving sustainable development, but should also be limited to a certain extent, in order to achieve sustainable development. Of course, it may be difficult to draw a clear borderline between information which should be accessible and which not. Issues of information safety when sending electronic messages are discussed in the next section.

3.1. Information, security and costs

In order to keep information safe, different methods can be applied. In this section the relation between costs and security of sending information in electronic form is discussed. In Table 1 the time needed to ensure security of information, costs and the level of security of different ways of transferring information is presented.

Table 1. Relation between costs and information security

Tool used for transferring information	Time needed to prepare security of information	Costs	Level of security
E-mail	none	none	none
Standard software tools	short	none (if freeware)	low
Advanced software tools	medium	average	medium
Hardware tools	short	very large	highest

Source: Platje and Trzmielewski, authors' own elaboration.

To what extent information has to be protected of course depends on the type of information we are talking about. In economic terms, it only pays to protect information which has value to an economic subject and the costs of protection are not too high compared to this value. E-mail is a mean of communication which is mostly used for informal exchange of

information and discussion [OECD, 1996, 92]. If standard e-mail is used, no costs are incurred and the level of security is none. Thus, e-mail will rather be a mean for transferring information with, generally speaking, a low economic value.

Standard software tools may be used to encode e-mails. Preparation time is relatively short. No costs are incurred when freeware, which can be downloaded from the internet, is used. Examples are Adobe Acrobat and Pretty Good Privacy (PGP). The first of these is a program distributed by the firm Adobe, which converts files into standard PDF (Portable Document Format). This program enables the blocking of certain functions, *e.g.* print, edit. In order to unblock these functions, it is necessary to enter the appropriate password. The second program carries out encoding of the contents of files, as well as e-mails. The level of security of Acrobat is relatively low when a poor password and appropriate decoding method is used. Although in general the level of security is low, higher security can be obtained by, in the case of PGP, using other keys/encoding methods. When a good method is used, decoding takes 2 or 3 days, or even less. When there is no information about the characteristics of the key, it can take several centuries to decode a key with 7 signs.

Advanced software tools, which are used *e.g.* to encode both business and government secrets, may be used to encode electronic documents to be sent between embassies, government agencies, security agencies, etc. The time needed to ensure security of information and costs incurred are greater than in the two cases discussed above, but the level of security is also higher. However, as the level of security is not very high, other methods should be used when the value of information is very high. In this case hardware tools may be used. An example is "Clipper", an old system that was used in the 1990s. In order to use this system, a card that encodes online is installed in the computer. Such a method is expensive, as specialised integrated circuits, specialised processors, special programs for processors, secrecy programming, etc. are used. An advantage lies in the fact that the preparation time is short and the level of security the highest of all four methods discussed.

3.2. Decoding a password

In this section some results of research carried out between October 2002 and February 2003 at the Wrocław International School for Logistics and Transport are presented. Using standard software tools, analytical methods for decoding documents that have to be sent by public channels were explored. An important question is to what extent are

documents safe from being decoded and how fast can a password be decoded. In other words, does a password make sense?

The research was carried out on a standard personal computer (550 MHz processor, 128 KB RAM memory), using Windows 98. Investigations were conducted on documents encoded with an 128 bite and 40 bite password, *i.e.* at the same level as used in popular internet viewers. Documents were created using a text editor and then transformed into PDF format. The encoding mechanism of the Adobe Acrobat was used in this process. The length of the password varied from 1 to 7 signs. The software used for decryption (decoding) is generally accessible on the Internet: Advanced PDF Password Recovery Pro ver 1.7 b84 (2001) from the firm ElmSoft Co Ltd. It was assumed that the person decoding a password or key does not have any information about the person or organisation that encoded the message and that "dictionary methods" are not used. If it were possible to use dictionary methods or combine, for example, dictionary methods and sociotechniques, then the time required to break the code could decrease by a factor of about a thousand. The investigations were conducted in series for span folding (only using signs from the Latin alphabet) using: capital letters; capital and lower case; capital, lower case digits and uppercase figures; all ASCI signs in the range 032–128.

Documents were encoded with a password where the combination of signs was chosen at random. In the 9 cases (out of 365 – in the case of a 128 bite key) where the time required to decode was assessed to be greater than 150 days, a mathematical algorithm was used to estimate this time.[2] It has to be mentioned that when proper programs are used, information about the encoder is available and "dictionary methods" are used, the time needed to decode 128 bite passwords declines by 50% or even more. The general results of the research are summarised in Table 2.

Table 2. Speed of decoding passwords – statistical results

	40 bite codes	128 bite codes
Mean rate of decoding (passwords/s)	86825	4345
Number of files encoded	375	365
Mean rate of decoding calculated mathematically (passwords/s)	86734	4302.14

Source: Research carried out at the International School for Logistics and Transport in Wrocław.

[2] If the program signals that the time required to decode the message is greater than 150 days, an estimate for the decoding time is based on the average speed of decoding (requiring 30 minutes) and the number of possible passwords in a particular set.

It should be noted that in any generally accessible decoding programme there are loops which slow down the programme [Hoffman, 1995]. Hence, these results do not reflect the real rate of decoding. Removing these loops would increase the rate of decoding a hundred-, or possibly thousandfold.

Figures 1 and 2 present the time needed to decode 128 bite and 40 bite passwords. D stands for only capital letters, M – capital and small letters, N – capital letters, small letters and numbers, S – capital letters, small letters, numbers and special signs (*e.g.* dots, commas), W – capital letters, small letters, numbers, special signs and spaces

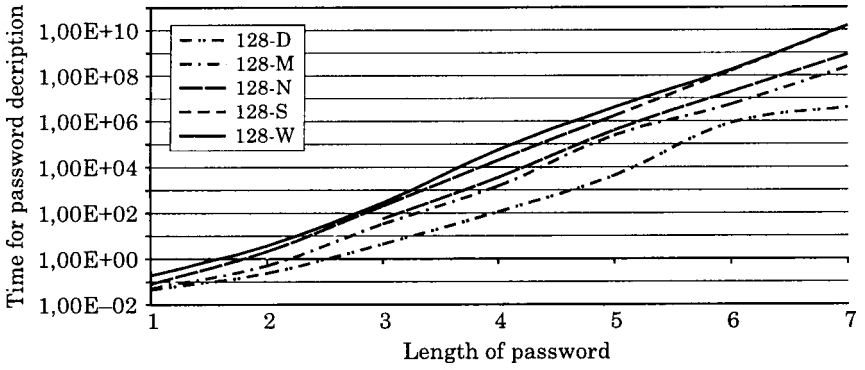

Fig. 1. Time needed to decode a 128 bite password

Source: Research carried out at the International School for Logistics and Transport in Wrocław.

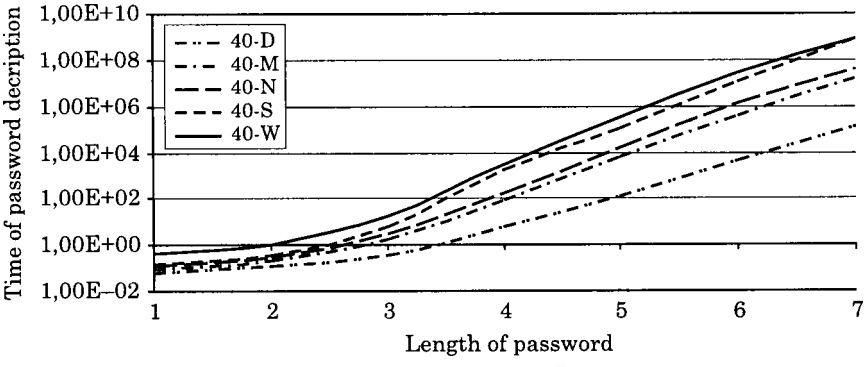

Fig. 2. Time needed to decode a 40 bite password

Source: Research carried out at the International School for Logistics and Transport in Wrocław.

Besides the research method used (Brute-force – ciphertext-only attack each possible password is checked in order until the correct pass-

word is found), more advanced decoding techniques exist such as: knowing plain text only attack, chosen plain text attack, adaptive chosen plaintext attack and chosen key attack. It should be noted that the time required to break a code rises exponentially with the length of the password. The number of signs permitted in the password is also important. For example increasing the number of permissible signs from 26 (only capital letters) to 95 (capital letters, small letters, numbers, special signs and spaces) – approximately 4 times as many signs – increases the time required to break a code by a factor of almost 10 000, from just above 10^6 seconds to 10^{10} seconds. One should also note the significant change in the time required to decode when the the code is changed from 40 bite to 128 bite.

4. Concluding remarks

Although access to information is important for sustainable development, arguments have been presented that sustainable development may require limiting access to information. For this reason electronic messages may be encoded. In general, better encoding systems are more expensive. Thus, the more valuable information, the more advanced methods are likely to be used for encoding.

When information about/from the sender of an electronic message is known, such as the type of information sent, personal characteristics, telephone number, habits, etc., it is relatively easy to get access to certified information using generally accessible programs and equipment. Specialists (*e.g.* secret services, industrial espionage) have more advanced techniques at their disposal. Furthermore, the faster the processor, the more easily a code can be broken. As the power of computer chips is still increasing very rapidly, one question is whether encoding technology can keep up.

Generally speaking, it is possible to decode any message. When a new encoding system appears, decoding methods follow very quickly. For this reason not only encoding systems are of importance. It is also important whether the sender of information is able to find out who gained unauthorised access, and whether that person can be persecuted. This depends on whether a legal framework exists that protects the sender of information from being "robbed", and whether these laws are enforced by police, judiciary, etc. In other words, besides proper encoding methods, an efficient institutional environment facilitates the protection of information.

Literature

Akerlof, G.A., "The Market for 'Lemons': Quality, Uncertainty and the Market Mechanism", *Quartely Journal of Economics*, 84, pp. 488–500, 1970.

Gubrynowicz. A., "Poland's Environmental Protection Commitments in the Light of Selected Multilateral Treaties", in: *Yearbook of Polish Foreign Policy 2003*. Warszawa: Akademia Dyplomatyczna MSZ –Wydział Wydawnictw, 2003.

Heyne, P., *The Economic Way of Thinking*, 8th ed.. Upper Saddle River: Prentice Hall, 1997.

Hoffman, L.J., *Building in Big Brother – The Cryptographic Policy Debate*. New York: Springer Verlag 1995

Konstytucja Rzeczpospolitej Polskiej. Lublin: Lubelskie Wydawnictwa Prawnicze, 1997.

Molho, I., *The Economics of Information – Lying and Cheating in Markets and Organizations*. Oxford: Blackwell Publishers, 1997.

OECD, *Integrated Advanced Logistics for Freight Transport*. Paris: OECD, 1996.

Platje, J., "Environmental Protection and Economic Development", in: Platje, J., Słodczyk J. (eds.), Economic and Environmental Studies 2/2002, *Environmental Challenges in the Process of Eastward Expansion of the European Union*. Opole: Opole University, 2002.

Platje, J., *Institutional Change and Polish Economic Performance since the 1970s – incentives and transaction costs*, doctoral dissertation. Groningen, 2004.

Poznański, K.Z., *Poland's Protracted Transition*. Cambridge: Cambridge University Press, 1996.

Rao, P.K., *Sustainable Development – Economics and Policy*. Oxford: Blackwell Publishers, 2000.

Sen, A.K., *Inequality re-examined*. Oxford: Clarendon Press, 1992.