EDRi response to EC consultation on the review of the Data Protection Directive

15 January 2011

Table of Contents

European Digital Rights
Rue Montoyer 39/3, B-1000 Brussels
E-Mail: joe.mcnamee@edri.org, http://www.edri.org

About EDRi

European Digital Rights, EDRi, is a European not for profit, non-governmental digital rights organisation. EDRi was founded in 2002 by 10 organisations (only NGOs may be members) from 7 European countries. Since then EDRi membership has grown consistently. Currently 29 organisations have EDRi membership. They are based in or have offices in 18 different countries in Europe. In addition 17 observers participate in the organisation's mailing lists and activities. We think of Europe in terms of the Council of Europe territory - not strictly its Member States.

EDRi's objectives are to promote, protect and uphold fundamental human rights and freedoms in the digital environment. Examples of such fundamental human rights are the freedom of expression, privacy, data protection and access to knowledge.

To this end, we strive to monitor, report and provide education about threats to civil rights in the field of information and communication technology. One of our recent awareness raising tools is the comic book "Under Surveillance", which we developed together with our international partners in a project funded by the European Union. Another example is our bi-weekly newsletter, the EDRi-gram, which just concluded its 8th year of high quality reports on digital rights in Europe.

We conduct policy research and offer the results to the public and to national and international bodies. Recent examples are our contributions to the European Commission's expert groups on RFID and on the Internet of Things, our responses to the European Commission and Council of Europe (CoE) consultations and our work as observers to CoE working groups.

Furthermore, EDRi and its members advocate at a national and international level by actively engaging with bodies such as the European Union, the Council of Europe, the OECD (EDRi was instrumental in CSISAC formation and recognition by OECD, the writing of the CS Seoul Declaration in 2008, whose endorsement is a requirement for CSISAC membership), WIPO and the United Nations as well as organising and participating in a number of conferences and public events.

EDRi also serves as a platform for cooperation and common activities, combining the influence, experience, knowledge, and research of its members. EDRi's activities are primarily driven and carried out by its members' representatives in addition to their national activities. Together EDRi members, observers and friends advocate and inform civil society, industry and the policy sector to uphold fundamental rights such as privacy and freedom of speech in the information society.

European Digital Rights
Rue Montoyer 39/3, B-1000 Brussels
E-Mail: joe.mcnamee@edri.org, http://www.edri.org

Introduction

EDRi is of the opinion that legal certainty, both for data subjects and data controllers, can be vastly improved by not having a directive on data protection, but a regulation. Currently, the lack of uniformity of the implementation of data protection legislation harms both data subjects and data controllers. It reduces transparency, since a data subject's protection may vary, depending on the location of the controller. Likewise, it adds to the administrative burden of data controllers since they have to adhere to varying regimes, especially when data controllers operate in multiple member states. This situation is exacerbated by widely varying legal, financial and human resources available to national data protection authorities in the EU – further reducing legal certainty for both citizens and data controllers.

Moreover, EDRi feels that the current regime lacks a sufficient risk-reward balance for data controllers to give them true incentives for taking the appropriate steps to ensure adequate protection of personal data. Especially in light of technological advances, the marginal costs of processing additional personal data is dropping towards zero, whereas the risks of any data being leaked, being incorrect or being used for other purposes than originally intended continue to grow exponentially and are not sufficiently borne by data controllers. Any review of the directive should take into account that, due to the relentless pace of technology, any risk not borne by the data controllers will fall on the shoulders of the data subjects.

Many of the suggestions made in the Commission Communication could, in fact, be reasonably understood to be part of the existing data protection framework. However, these rights are not enforceable by some or all EU citizens due to lack of consistency of understanding of the directive and lack of resources of national DPAs. We fear that not enough has been done to learn from and rectify the existing implementation problems. Unless and until this is done, there is a huge risk that privacy rights will become more uncertain for citizens and their respect will become more of a burden than an asset for public and private data processors.

1. Harmonisation of definitions

There is an urgent need to clarify the definitions in the 1995 Directive. It is impossible to have a harmonised EU approach to protection of personal data when there exist significant differences between the meaning of "personal data" between one country and another.

The EMI Records & Ors -v- Eircom[1] Ltd provides excellent insight into the range of problems in this regard and points to the general lack of legal certainty for European citizens concerning their privacy rights. Not alone was the Irish DPA unable to give an opinion in this case, the court ultimately ruled that IP address data collected for the purpose of identifying persons was not personal data, because it was not directly identifiable by the collector of the data. This ruling is even more absurd when read in conjunction with recital 12 of the directive, which states that, to determine whether a person is identifiable, account should be taken of "'all the means likely reasonably to be used either by the controller or by any other person to identify said person."

The Irish case comes twelve years after the implementation of the directive and numerous examples of clear guidance on relevant questions such as Opinion 4/2007 from the Article 29 Working Party. The lack of participation of the Irish DPA in this case, the contradiction between accepted understandings of the concept of "personal data" in this case with accepted norms and the lack of response/criticism from the European Commission provide a perfect case study of what needs to be avoided in the review of this directive.

In this regard, EDRi would like to point out that the recent proposals of the Federal Trade Commission (FTC) in the United States on what constitutes personal data might be helpful in this regard. The FTC has defined it as "all (consumer) data that can be reasonably linked to a consumer or a computer or another device". We've bracketed the "consumer" part since this is obviously tied to the FTC's limited competences in the US context. The advantage of a definition like this is that it will prevent the recurrence of disputes on whether or not network addressing schemes are personal data every time a new scheme becomes mainstream.

EDRi is also concerned about the lack of clarity regarding the concepts of "controller" and "processor". On a basic level, these terms lack clarity in the directive and are made much more unclear in the context of international organisations, which is further exacerbated by inconsistent interpretations between Member States. This is ultimately detrimental to the legislative power of the directive.

We also believe that action is needed to ensure a harmonised approach to purpose specification and purpose limitation. An urgent review of current practices with regard to public sector and research exceptions is also needed. It is wholly unacceptable that widespread breaches of the directive are still in force at this stage in the lifecycle of the instrument.

Finally, particularly in an Internet context with often long and unclear privacy policies, and as clearly illustrated in the Eircom case above, the issue of consent should be comprehensively addressed.

1 http://www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d8840802577070035082f?OpenDocument

2. Strengthening individuals' rights

EDRi welcomes the Commission's intention to consider how to ensure a coherent application of data protection rules. We believe that, even without the technological change that has happened since the adoption of the 1995 Directive, this would have been necessary, due to the profound differences in implementation of the directive across Europe.

Technological developments since 1995 create the need to strengthen individual user's rights in two key ways:

a. Minimising harm from the potential of new technologies

Data processing by states

New technologies have led governments to increasingly look to technology both to undertake pre-existing policing activities (via speed cameras, number plate recognition, etc) and to create new policing activities, such as "profiling" of individuals to identify alleged patterns of behaviour that can identify possible illegal activity. Electronic patient records, e-government systems and surveillance systems can and increasingly are being used for this purpose. In addition, data storage and processing obligations, such as through the directive 2006/24/ec on retention of communications data offer information (such as mobile location data) that was not previously available to law enforcement authorities.

The fact that the Council of Europe saw fit in its Recommendation on profiling (CM/Rec(2010)13) to grant a wide-ranging exception to states to ignore its provisions on lawfulness, data quality, sensitive data, information and rights of data subjects gives a very clear warning of the imminent dangers that such processing pose to fundamental rights in Europe and globally. In the words of the preamble of the Recommendation itself, the "use of profiles, even legitimately, without precautions and specific safeguards, could severely damage human dignity, as well as other fundamental rights and freedoms, including economic and social rights".

Within the context of the new horizontal nature of the directive, it is crucial that the scope for states to indiscriminately process and link data be limited to what is strictly necessary, taking due account of the privacy and security costs of such measures.

Data processing by companies

- Profiling

There is now greater potential for storing personal data for advertising purposes than ever before. Whereas the targeting of traditional advertising is quite general (children's products during TV shows aimed at children), processing of data generated in the context of internet browsing permits advertising to be served that is much more specific to the individual. This has

lead to hugely profitable markets - Google's revenues in 2009 were $23 billion[2] while Facebook reportedly[3] generated $1.2 billion in the first nine months of 2010.

The monetary value of such profiles suggests that, in addition to the fundamental right to privacy, the fundamental right to property, as described by the Charter of Fundamental Rights is also at stake. The current situation, where consumers are being profiled through means (cookies for example) of whose existence - let alone their profiling purpose - they are frequently unaware needs to be addressed in a way which ensures citizens' rights.

b. Measures to strengthen users' rights

- Privacy enhancing technologies

While the Commission has made some valuable efforts to increase the profile, development and use of privacy enhancing technologies, far more needs to be done. This should be a key component of awareness-raising activities undertaken by the Commission to make citizens more aware of their rights, the dangers of not protecting their rights and the tools to maximise privacy.

- Increasing transparency for data subjects

EDRi supports all of the measures currently listed as under consideration by the Commission in its Communication. However, we have seen from the existing directive that huge variations in implementation are the result when general principles are not followed up with very precise guidance (and sometimes even if they are). Consequently, we would encourage the Commission to take this experience into account when developing what it refers to as a general principle of transparent processing.

We welcome the Commission's suggestion for specific obligations on the type of information to be provided and, in particular, on modalities of communication. In this context, standard privacy notices could also improve transparency, particularly if they build upon existing best practice. Additional protection for children is welcome but this should be built on a strong general framework for privacy.

EDRi would in general like to see that the right of data subjects to demand disclosure to them of any personal data processed by data controllers to be free from any administrative burdens. EDRi is of the opinion that if the costs of any such disclosure are prohibitive to a data controller, the data controller probably never had a legitimate interest in the data processing to begin with. It therefore is unreasonable to have a data subject pay in any way for such disclosure.

- Data minimisation

Public authorities have failed to provide examples of best practice in the EU. From health databases to smart metering and publicly-funded transport ticketing systems, there has been a

2http://investor.google.com/financial/tables.html
3http://news.yahoo.com/s/nm/20110106/wr_nm/us_facebook_goldman

fundamental failure to ensure proportionality, privacy by design and data minimisation.

The role of public authorities is to ensure best practice - from intelligent transport to unproven "health and safety" technologies such as national health databases. The "Summary Care Record" system in the United Kingdom failed to make efforts to learn from less intrusive and dangerous systems elsewhere in the world and placed the onus on patients through an opt-out system. There is far too big a gap between the policy statements of governments regarding protection of personal data in the private sphere and the massive collection and interlinking of data in the public arena.

- Rights of access, rectification, erasure or blocking of data, the right to be forgotten and data portability

EDRi warmly welcomes the proposals from the European Commission on these points. Nonetheless, we are concerned that these rights already lie in the existing framework and that, without analysis of why these rights are not currently being respected, the Commission may not be equipped to ensure their respect in the future. To a considerable extent, these rights are contingent on effective implementation of “privacy by design”, without which public and private bodies will be able to claim that respect for the rights is too onerous. The current use of IPv4 addresses is a good example of this – a similar lack of privacy by design in the rollout of IPv6 would be far more damaging.

- Data controller responsibility

The focus from the Commission to improve the framework within which data controllers understand and respect their obligations is an important step in the right direction. However, most of the measures proposed are not new and more effort needs to be made to fully understand why, for example, PETs and privacy by design have failed to achieve their potential up until now. Implemented properly, the Commission's proposed introduction of an obligation for privacy impact assessments should help ensure that privacy concerns are built into every part of the lifecycle of a product or service. This should be bolstered by the mandatory appointment of a data protection officer with, from the outset, “mandatory and harmonising the rules related to their tasks and competences”.

- Self-regulatory initiatives and certification schemes

There is no question that self-regulatory initiatives can be useful in supporting citizens' rights. However, it would be a mistake to expect too much from such systems. Commercial trustmark schemes suffer from a tradeoff between being sufficiently thorough (which requires an often off-putting level of investment in terms of time and oversight) and being sufficiently lenient for companies to be willing to join (which can undermine the credibility of the system). We would therefore urge the Commission to be extremely cautious in this regard and to ensure that no self-regulatory initiatives or certification schemes be permitted without adequate oversight and legal underpinning. In short - self-regulatory initiatives can work but the difficulties involved must not be underestimated.

- Breach notification

Following the adoption of a breach notification obligation in the revised directive on Privacy and Electronic Communications, the expansion of this obligation to all data processors is a logical and necessary step. With one caveat however, EDRi feels that breach notification to data subjects is much more important than breach notification to DPAs. It is data subjects that are most likely to suffer adverse effects from a breach, for example by way of identity theft. Data subjects should be enabled to mitigate any such adverse effects, notification is essential for this purpose.

European Digital Rights
Rue Montoyer 39/3, B-1000 Brussels
E-Mail: joe.mcnamee@edri.org, http://www.edri.org

3. Updating the Directive: taking new technologies into account

EDRi is of the opinion that any review of the directive should take into account three major trends:

I. The exponential growth in personal data processing capabilities
II. The further disconnect between data processing and physical location
III. The internet of things

I. The exponential growth in personal data processing capabilities

The exponential growth as such is not a new phenomenon, if anything it should have been taken into account during the drafting of the current directive. It is caused by the incredible price erosion of computing power, connectivity, data storage and sensors. This has already created vast potential for the abuse and negation of the individual right to privacy and is very likely to continue doing so.

As stated in the introduction, the risk-reward balance for data controllers is skewed and any review of the directive should take the relentless pace of technological change as force for this balance to become more unhinged into account. Therefore, at the very least, EDRi is in favour of measures that will make the public disclosure of breaches of security mandatory - indeed, this is a logical and inevitable step, following the review of the 2002/58 Directive. Any lack of disclosure of such breaches should result in the liability of offending data controllers towards the data subjects involved. Moreover, we strongly advocate measures that will allow data subjects to hold data controllers liable if they have not taken reasonable steps to prevent leaks. This is both a matter of fairness and of providing the right incentives to data controllers to make more rational cost-benefit decisions on the processing personal data.

II. The further disconnect between data processing and physical location

Another long-term trend is that data processing is no longer tied to geographical location in the traditional sense. This was already the case in the mainframe era, but has become more acute with so-called cloud computing. As such, a number of questions about jurisdiction of data that is moved back and forth between various jurisdictions become painfully acute. EDRi is in favour of an approach that takes a functional view on this. For example: data that is transmitted through various jurisdictions by way of an end-to-end encrypted connection should not be treated as data that had become subject of all jurisdictions involved, but only of those at the endpoints of the connection. Similarly, data that is stored within the European Free Trade Area, but is administered from outside it, should be treated as having been de facto exported data. Most issues in this respect can be solved by clarification of the terminology, and not necessarily by fundamentally changing the current framework. There are nonetheless two fundamental change that EDRi would suggest:

a) Any entity that is active on the common market and actively markets its services on the common market, for example by using languages used within the common market and

pricing its services in Euros should be obliged to have a legal presence within the common market which can serve the role of data controller.

b) Abolition of the notion of joint controllership. Given the fluidity of relationships in the supply chain of cloud computing services, it should be clear which data controller can be held accountable by data subjects and which DPA. Joint controllership creates legal uncertainty for both data subjects and data controllers. To prevent controllers from 'shopping' for the most lenient jurisdiction, the directive should obviously become a regulation.

III. The internet of things

The result of the earlier mentioned trends of ever cheaper data processing and collection is that more and more everyday objects become sensors that are connected to a wider network of systems. Prime examples of this are obviously smart metering and so-called domotics. EDRi considers it very unlikely that the ultimate effects of this trend can be foreseen. However, it is easily foreseeable that this will lead to ever more collection of personal data. As such, it will become impossible not to be under surveillance to at least a certain extent. In order to provide safeguards for data subjects, EDRi would be in favour of the Commission taking the opportunity of the review of the Data Protection Directive to enhance data subject's right to access to data and to make it clear that privacy overrides any intellectual property rights the producers of embedded systems claim to have. This includes mandatory disclosure of data being stored and/or transmitted and the interfaces through which this data is accessible. Likewise, EDRi would like to see a reasonable expectation of consumers of the data security of products and services to be put on the agenda. The internet of things is also an area that can be expected to provide future conflicts on what constitutes 'personal data', which is one of the reasons EDRi finds the FTC definition so helpful in this regard.

4. Increasing legal certainty and providing a level playing field for data controllers

EDRi is also of the opinion that the current directive provides so little enforcement power to DPAs, especially on the subject of international data transfers, that there is a strong incentive for data controllers to ignore the instrument. For example, the current hosting costs in Western Europe for a single server are about 600 Euros per month, of which 200 Euros are the labour costs for systems management. If the same server is either entirely hosted in India or managed from India, which in either case amounts to an international data transfer, the labour costs drop to 20 Euros per month. This obviously provides a strong incentive for moving the labour to India, with the only risk that it must be moved back in case a DPA finds out.

The aforementioned example shows that a lack of actual power for DPAs leads to distortion of the common market, since larger service providers are more likely to be able to move operations to low-labour countries. Giving real power to DPAs will increase legal certainty and provide a more level playing field for data controllers.

Another area in which legal certainty is lacking is that of data security. So far the Article 29 Working Group, as well as the individual DPAs, have tried to provide guidance to data controllers on the lofty principles of section VIII of the directive. It nonetheless has resulted in a lack of clarity and legal uncertainty. EDRi would prefer the inclusion of a mechanism of a yearly review at the EU-level to provide data controllers information on what constitutes "appropriate technical and organizational measures", which obviously change over time. To give an example: the last publication from the Dutch DPA on this subject that provides concrete information dates from April 2001. Given that the Dutch DPA has been one of the more established and active DPAs, it is obvious that the pace of technology has outrun that of the DPAs in this regard and that data controllers are more less operating in the dark.

5. Reducing the administrative burden

EDRi is of the opinion that the obligation for data controllers to notify their DPA of the data processing is a diversion from the real issues, namely whether the data processing should take place to begin with and what appropriate measures should be taken to prevent processing outside the scope of what the directive allows. Therefore, EDRi is in favour of removal of the obligation to notify DPAs of the data processing. This both reduces the administrative burden of data controllers and frees up capacity at DPAs for activities that materially contribute to privacy for data subjects.

6. Revising the data protection rules in the area of police and judicial cooperation in criminal matters

As we have seen in numerous examples (SWIFT and PNR being just two examples) of data collected for private purposes being used – and exported – for police and security cooperation purposes, it is no longer logical or feasible to have a legal framework which keeps the former "pillars" of EU instruments separate for data protection purposes. It is therefore essential to extend the protections offered in the policy area previously covered by the "first pillar" into the area of police and judicial cooperation.

A significant effort needs to be made to implement the concrete principles of Council of Europe Recommendation R(87)15, which is the minimum price that should be paid for the levels of police and security cooperation that are currently demanded and enacted within the EU and between the EU and third states.

In order to ensure respect for the fundamental right to privacy, increased police and security cooperation must be set at the highest level required by any of the Member States' constitutions, and by European human rights law. The Council of Europe Recommendation on the use of personal data in the police sector can be used as a basis, on the obvious assumption that it is effectively respected, which has not always been the case up until now.

The principles of the directive must be effectively applied to all of the areas that were previously covered by the third pillar, including those which were previously exempted under Article 13.

7. Clarifying and simplifying the rules for international data transfers

EDRi is of the opinion that having a regulation instead of a directive would provide a major step forward regarding the clarity of the rules for international data transfers. EDRi is also of the opinion that the current 'safe harbour' exceptions result in an opaque and unaccountable situation for data subjects. At the same time, EDRi feels very strongly about retaining the base principle that personal data should not be exported to jurisdictions without safeguards that are materially similar to those within the European Free Trade Area. As such we would like to see the inclusion of a grant of power to impose fines in this respect to DPAs.

8. A stronger institutional arrangement for better enforcement of data protection rules

As pointed out several times above, the volume of personal data being processed has grown, and is still growing, exponentially. So far enforcement of data protection rules has relied heavily on DPAs, whose resources have not grown exponentially in the meantime. Most DPAs have had to cope with limited funding, staffing and powers. One could even argue that, given the prominent role DPAs have in enforcing the data protection rules and the limitations that have been imposed upon them, the current institutional arrangement has been more of a hindrance than of an enabler for the enforcement of data protection rules.

This review of the directive should therefore give DPAs the mandate to:

a) publish any review of data controllers they undertake at the start of such a process
b) give DPAs the power to fine data controllers that have been found to be violating the directive and
c) give DPAs the power to have third parties audit data controllers at the expense of data controllers when a DPA has reason to suspect violations by the data controller.

The level of the fines should obviously be meaningful and not be limited to symbolic amounts. The experience of many DPAs is that data controllers tend to take an uncooperative position during reviews until the review is about to become public. As a result of this, the DPAs are forced to spend their already limited resources in an inefficient manner. Furthermore, DPAs cannot possibly expect to retain the technical expertise required to perform audits of data controllers at an adequate level and on a meaningful scale. As said before, the relentless pace of technology at a sometimes asymptotic rate cannot be reconciled with the notion of DPAs with limited resources. It therefore stands to reason that this burden is borne by the parties who benefit the most from the data processing, namely the data controllers.

9. Applicable law

As stated earlier in this document, having the possibility of joined controllership, and therefore multiple applicable laws, is untenable. Data controllers should be allowed to choose a jurisdiction within the member states whose DPA has the authority to regulate the data processing. This would both reduce an administrative burden to data controllers and would clarify the position of data subjects which themselves, thanks to the common market, are moving back and forth between member states in ever larger numbers. The best way to achieve this is having a regulation instead of a directive, with the option for data controllers to chose the applicable member state law, and therefore DPA. The position of data subjects can be safeguarded by either having their requests to other DPAs being passed on to the DPA chosen by the data controller, or other DPAs acting on behalf of the DPA chosen by the data controller.

10. Property rights

The EMI Records & Ors -v- Eircom Ltdcase raises some important questions that need to be clarified by the Commission as part of its wider approach to data protection. As mentioned above, the Irish judge appears to have taken the view that processing of personal data which was:

- not a necessary part of the service being provided for its consumers;
- not subject to any specific or implied consent from the data subjects and
- obtained from third parties that hand not received any specific or implied consent

was legal, on the basis that it was within the legitimate interests of Eircom, which has to be "act, and to be seen to act, as a body which upholds the law". In other words, any data processing which could be argued as potentially upholding any law is legitimate. Indeed, even processing which would not potentially uphold any law would also be legitimate, if the data processor could argue that it appeared to be a mechanism to uphold the law.

The European Commission's Communication on application of Directive 2004/48/ec (COM(2010)779) final appears to endorse such an approach. It appears to seek to propagate the myth that the European Court of Justice urged a re-balancing of the right to privacy and the right to property – ignoring the fact that the Court did not say, or suggest, that any such rebalancing was necessary. Even more strangely, it suggests the fundamental right to privacy should not be used as a defence against any measure which might serve to enforce property rights.

There is, however, an obvious and logical difference between data which is clearly personal and subject not only to protection in the Charter of Fundamental Rights, but also the European Convention on Human Rights and the International Covenant on Civil and Political Rights and the more vague concept of property rights. The only possible approach is for courts – and not private companies, as in the Eircom case – to assess what is necessary and proportionate in any given case.

There is also an obvious and logical difference between specific privacy rights and the rights that may be upheld on the basis of questionable evidence. Cases in both Germany and Denmark were overturned on the basis that IP address data provided by intellectual property owners was not reliable.

A specific fundamental right cannot be "balanced" against fishing expeditions to find "evidence" that would seek to defend another right. The right to privacy cannot be balanced against a data processor's interest "to be seen to act" to enforce any given law, it cannot be balanced against the willingness of the holder of another right to impose specific policing mechanisms.

Summary and conclusions

To summarize and conclude EDRi's position, the review of the directive should include

- harmonisation of definitions that would both address the divergence in the jurisprudence in the various member states and prevent predictable conflicts whenever a new technology becomes relevant.
- include measures to counterbalance the exponential growth in the volume and nature of data processing, including breach notification to data subjects as well as liability for breaches towards data subjects. This should also include measures regarding the ever growing data processing in so-called embedded systems, the so-called internet of things.
- a conversion to a regulation instead of a directive, which would increase the legal certainty and provide a level playing field for data controllers as well as reduce their administrative burden, which can be even further reduced by removal of the data processing notification obligation. In addition to this, it would clarify and simplify the rules for international data transfers.
- an implementation of the concrete principles of Council of Europe Recommendation R(87)15 in the data protection rules in the area of police and judicial cooperation in criminal matters.
- a fundamental extension of the powers of DPAs to fine violators of the directive as well as to have data controllers bear the financial burden of audits by the DPAs.
- make it clear that the legitimacy of the need for rightsholders to gather evidence of infringement ends when such gathering of evidence is done in such a way that the directive is violated.

European Digital Rights
Rue Montoyer 39/3, B-1000 Brussels
E-Mail: joe.mcnamee@edri.org, http://www.edri.org