Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Internet and privacy : any conclusions

Poullet, Yves

Publication date:
1999

Document Version
Publisher's PDF, also known as Version of record

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 1999, *Internet and privacy : any conclusions*..

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 18. Mar. 2025

YP R88

Internet and privacy : any conclusions

Yves Poullet

1. the 1st ECLIP seminar was dedicated to the privacy problems derived from the multiple e commerce activities.

In these conclusions, I would like to summarize the presentations of the speakers and the multiple interventions of the audience and perhaps suggest new ideas and trails of research around three points :

- the first one underlines how new actors and, new technical possibilities are creating new risks and privacy threats ;

- the second one does envisage the regulatory solutions : how Internet does challenge our legal framework, claiming new basic principles but also suggesting certain audacious interpretations in order to cover new features.

- the third one would like to introduce new criteria to evaluate the selfregulatory solutions and privacy enhancing technologies.

I. New actors, new possibilities, new risks

2. The large number of actors or to be more precise of functions, intervening in the electronic transactions is definitively an important factor we have to take into account in our analysis.

Beyond the actors directly involved in the electronic transaction : the « customer » and the « sellor » (in the broadest sense, sofar as the sellor might be an administration, or a web site delivering informations and publicity without concluding commercial transactions), other secundary actors have been identified : the internet Access provider, the carrier, the Internet service or hosting provider, the web sites offering search engines, the payment gateways (clearing networks) and banks.

The need to create trust and confidence in the electronic commerce does suggest the intervention of a third category of actors : the certification authorities, the trusted third party and also auditor labelling the web site following different criteria (K. De Baere).

A this opposite, a fourth category has been denunciated by different intervenants : the « not thursted third party » (NTTP) (J-M. Dinant). So, the cybermarketing companies are processing data about the use of the web through cookies and invisible hyperlinks between them and visited web sites. So certain web sites through the « web-

spoofing techniques » (J-J. Quisquater) are creating for the web users the illusion to be connected to their favourite web site, and collecting then the data generated by them.

Finally, the discussions have been underlined the presence of a fifth category (J. Dietl, J-M. Dinant) : the software editors companies, especially the browser producer. It is quite important to take into account the technical features of the webbrowser in order to know exactly which kind of flows they are generating (e.g. automatic sending of cookies) or permitting (e.g. possible hyperlinks without preliminary notice to the websusers).

3. The second task of the research will be to identify clearly the multiple processings existing taking into account the multiple data, the various actors and the different steps, going from the simple presence of a company on a web site to the conclusion, performance and payment of a service or a good through electronic means. The following schema (J-M. Dinant) is a first representation of the data flows occuring in an electronic transaction.

4. A third task not yet undertakes, will be definitively the analysis of the actors' practices and eventually the contractual relationships the different actors might have between them.

So, to what extent, the IAP is retrieving or not all the data generated by their customers not only in order to have a better statistical knowledge about the use of its services but also to profile them ?

Which kind of transactions are existing between the cybermarketing companies and from one part, the different web sites creating an hyperlink to them and from the other part to the companies interested by knowing the web user profile ?

The achievement of this task will be made easier in the context of ECLIP, by the fact that the analysis of certain ESPRIT projects like AIMEDIA will reveal these practices.

II. E. Commerce and Privacy : a challenge for the regulatory solutions

5. Number of questions have been raised in that context. Perhaps, it would be possible to summarize these as follows :

- To what extent, the regulatory solutions (in the context of the workshop, we have considered only the two directives, the general and the Telecom ones) are challenged by the new data practices created by the use of the Internet techniques ?

- To what extent, through audacious interpretation of the regulatory framework, it would be possible to cover these new practices ?

- Thirdly, would it be possible to use other legislations than those strictly connected with privacy questions, telecom directives, consumer protection legislation in order to enhance privacy protection.

- Finally, do we need new concepts or principles in order to regulate Internet ?

A. The main challenges

6. As regards the identification of the challenges, certain remarks have been adressed (S. Louveaux – R. Julia – P. Grimalt – I. Walden).

The growing international or global character of the E commerce and therefore the multiplication of T.B.D.F. underline the need to take seriously into consideration the provisions there about (art. 25 Directive). What does mean « adequate protection » and which kind of contractual arrangements (Directive, art. 26) are we accepting in that perspective ? Could we consider that notwithstanding these provisions, an european judge might argue that « privacy protection » is of international public order and so deny any application of less effective foreign data protection ?

7. The multiplication of intermediaries in the data flows generated by E commerce (see, above 2) underlines the need to regulate their liability in case of privacy infringements of websites. Does the future directive about the liability for online services provide an adequate solution in that sense ? In that perspective, it has been underlined that the « reasonable » means to have cognizance of privacy infringements and to avoid them not only on a curative but also on a preventive manner must be defined. The concerns about the fear of an « overcensorship » of the intermediairies and about the need to have « recourse » possibilities for accused web sites before « independant » magistrates have been expressed.

8. Finally, the interactivity of the network does suggest an increasing role of the consent. The web user is enabled at each moment to remain or not anonymous to interup a website visit, to refuse or not the delivery of certain data, to accept or not certain practices, etc. All these possibilities are supposing the respect of a free, explicit and informed consent. In regard of this aspect, a lot of questions have been raised : to what extent, can we consider that the web user is informed in case of publications of the privacy practices on a F.A.Q. webpage. Is the consent free if the website in a quasi monopolistic situation, does not provide other solution than the sending of disproportionate data to obtain the service proposed. How, can one be sure that the consent is explicit as regards certain characteristics of the processing (e.g. the processing) is requiring transborder data flow or is pursuing different purposes presented as a undissociable block)?

B. Towards an audacious interpretation of the D.P. directives

9. Certain speakers (particularly S. Louveaux) and intervenants during the virtual litigation discussions have underlined the extensible interpretation of the data protection legislation concepts and provisions to solve new privacy threats in an Internet context. Amongst the various examples given, I will take again only three :

So, the concept of personal data (Dir. Art. 2) might be extended to certain data collected by cookies, so far they permit to sketch user's profiles (what a web user is doing) even if the identification of the web user as physical person is impossible. The remark following which a marketing company in the traditional world, is more interested to a potential customer's profile than to his identification as physical person is quite convincing in that perspective.

The interest of a broad interpretation of the provisions about the right to object (Dir. Art. 14) and about the « unsollicited calls » (Telecom Dir. Art. 12) might lead to grant to the web user and absolute right to forbid any hyperlinks to cybermarketing companies and to restrict certain uses of his websitepages in the context of automated research proposed by search engines.

The possibility to apply the art. 4.1.C. of the directive provides the application of E.U. member States legislation in case of processings making use of equipment located in Europe) in case of processing generated by cookies installed on the terminal equipment of the browser was considered as noticeworthy.

C. Beyond privacy regulations

10. During the discussions around the virtual regulation, certain intervenants have suggested that « consumer protection » regulation might also be of some help to solve privacy problems. The main interesting example was the « liability for defective products » directive. To what extent, a webbrowser allowing certain privacy infringments (J.M. Dinant) as the cookies' reception and sending without prior notice is a « defective » product. Other interesting remarks might be deduced from the « distance selling » directive as regards the right of the Web user to object to unsollicited e mail messages.

An other trail might be followed founded under the Telecommunications regulatory framework. One knows that « privacy protection » is one of the essential requirements to be checked to approve terminals equipment. To what extent, would it be possible to regulate the technical features of the web browser (e.g. the automatic sending of cookies) on that legal basis ?

D. Towards new D.P. concepts and principles

11. S. Engel has suggested that the privacy risks created by the use of technologies of information and communication in the e.commerce context require the adoption of new data protection principles. Three principles have been evoked in that context.

- the first one is the « data minimization ». This principle means firstly that each time and sofar personal data are not required, the right to stay anonymous must be offered to the Web (including regards the means of payment) user ; secondly, it implies that no more personal data will be processed than strictly necessary.

- the second one is the « integration of the functionnalities of the technology » in order to implement the data protection principles. The applications of this second principle are various and noticeworthy. It means that each time, the same technology than these used for collecting or processing data might be viewed as a way to implement even to enhance the data protection principles, the technology must be configured in that sense. So, the right for the webuser to be correctly informed about the website privacy practices might be implemented through website pages placed at first cast of the website or by hyperlinks to the codes of conduct respected by the website right for the webuser to have access to his own data or to object to processing for commercial purpose might (opt-out) be excercised electronically. Acoording to the same principle, one can imagine that through certain labels (no robot, no spam) the webuser might forbid automatically the use from one hand of his name as keyword for search engines or from the other hand of his e mail adress for the sending of unsollicited e mail.

  A lot of other examples might be given, particularly as regards the possibilities to ensure a free, explicit and enlighsted consent by technical means.

- the third one is the « enforcement of the legal position of the person concerned », that means that a certain number of initiatives must be taken in order to make transparent and enforceable through on line techniques, the multiple rights of the webuser. Beyond what has been already said under the 2d principle, it must be ensured that the access to the official or not official data protection authorities in case of complaints will be ensured.

  So far as a public registrar containing the notification of the website practices does exist (art. 17 of the directive), an hyperlink to this public registrar must be integrated and a clear indications of this possible hyperlink has to be indicated in front of the website. So the web user might have automatically a view about the content of the notification done by the website data controller or in case of missing hyperlink know that notification has been done.

  This hyperlink might be withdrawn if the website practices do no more comply with the practices notified.

  Finally, vade-mecum explaining the privacy risks, the privacy duties of the website data controller and the rights of the webuser as data subject must be broadly diffused including through Internet and the D. Protection authority must be present on the web through interactive, documented and updated website.

III. Some considerations about self regulation and privacy enhancing technologies

12. The question of self regulation and privacy enhancing technologies as potential ways for protection of privacy has been extensively analyzed and discussed during the workshop.

As regards PETS, considerations about P.3.P. (J. Dietl) and techniques of encryption and anonymisation (J.J. Quisquater) have been developed.

J. Berleur has described the main characteristics of the multiples existing codes of conduct and their poor content as regards privacy issues. K. De Baere has developped the belgian project called Trust2, which provides a system of global labellisation of websites practices. By «global labellisation », we mean an audit about the main aspects of a website practices (compliance with privacy, security, fiscal, consumer protection, ... requirements).

A. Preliminary remarks

13. Certain remarks must be adressed before to propose a list of criteria in order to evaluate PETS and self regulatory solutions.

About the P.3.P. beyond remarks about difficulties to have a good terminology and a sufficiently sophisticated system to encompass all situation it has been fundamentally underlined that the shift from regulatory a priori solutions to the contractual paradigm (everything is negotiable) does represent a real danger for privacy. More generally speaking, it has been asserted that a « Human Rights » approach that is to say the fact that Data Protection is a constitutive element of a democratie Society implies the need to ensure Data protection by legislation. That conclusion does not mean that PETS (or self regulation) are not interesting as complementary ways to protect privacy but never they can be viewed as a substitute.

Other remark : the multiplication of self-regulatory solutions might be a source of confusion for the web user. In that context, it has been pleaded to have common european label and that the D.P. authorities would be envolved in the procedure for defining the label's requirement in order to access the compliance of these self-regulations with D.P. principles.

B. Criteria to assess the quality of the technical or selfregulatory measures for Protection of Privacy

14. The reflections laid down hereinafter aim to propose three criteria in order to evaluate the non regulatory privacy measures derived or not from a legal framework. As it will be underlined, it is quite clear that these criteria will be differently in these two context. In the first case, the self regulation must be viewed as a ancillary way to protect privacy and the most important question will be its compliance with the legislative requirement as expressly provided by art. 27 of the Directive. In the second case, the self regulation is a "substitute" and the question is then: "Is this substitute offering an "adequate" protection to take again the works used by art. 25 of the Directive?"

Anyway, in both cases, the assessment of the code of conduct will have to follow three criteria

- legitimation as regards the authors of the code;
- conformity as regards its content;
- effectiveness as regards its enforcement.

The three criteria are explicited as follows.

a. The legitimation

15. The first question to be raisen v.a.v a self regulation is the legitimation of its authors ! Who is promulgating the code of conduct ? Who has defined the technical standards ? To be more precise : after which kind of procedure, has the self regulatory mechanism been adopted. At our opinion, a self regulation might be acceptable only if all interested parties (that means not only the data controllers' representatives but also the data subjects' points of view have been taken into account). This envolvement might be ensured through different ways (e.g. by public hearing) but it must be checked if the procedure utilised to adopt the self regulation was at that point of view, sufficiently open and transparent. This requirement is absolute in case of non existing legislative framework.

b. The conformity

16. To what extent, is a self regulation complying with the D.P. principles? This question is crucial. Indeed, what will be checked by the auditor in case of demand of a privacy label adressed by a web site data controller ? What does mean in case of technical standards to be a privacy complying techniques ? In case of existing legislation, this conformity's examination might be simple but in the other cases, the solution to this question is rather intricate. However, one might consider that certain D.P. principles are internationally recognised :

1. The data subject's right of access and rectification;
2. The purposes limitation and the need for a social justification;
3. The data proportionnality ;
4. The security measures' requirement

c. the effectiveness

17. Compliance with data protection principles and legitimation of the authors are not sufficient. The third criteria intends to measure the effectiveness of the selfregulation. Three subcriteria might be distinguished on that point.

- <u>the awareness and userfriendliness of the selfregulation</u>

Questions like the broad (or not) publicity and the easiness of access to the content of a code of conduct, as the userfriendliness of privacy enhancing technologies (e.g. Is the blocking of cookies' sending a time consuming operation ? Are the anonymisation's techniques easy to practice) must be raised. In case of PETs, the problem of their costs and their availability on the market for a webuser must be checked attentively.

- <u>the accessibility, quality and investigation powers of the controllers</u>

It is quite important that the authority in charge of the respect of the self regulation might be easily accessed by the web user , on a affordable cost a better gratuitously, that this authority is neutral and can act independantly of

the data controllers. This authority must be equipped with real powers of investigations and finally, its dealings must be transparent (for example, via a report accessible to the public or by the publication of its decisions).

- the need for effective sanctions

It is quite clear that other sanctions than the penal ones might be envisaged and are often more effective, so the blocking of a website, the withdrawal of a label, etc. The only criterion must be : are the binding sanctions promulgated by the self regulation sufficiently deterrent to prevent the non respect of the D.P. principles?

Conclusions

17. Recently, I was told by an american friend in a provocative manner. In Europe to regulate Internet, you have nice legislations, you have created bureaucratic data protection authorities but amongst the population, there is no privacy concerns and the protection you are offering is purely theoritical. In US, the privacy concern is very high, we have effective selfregulation and technical tools have been developed to solve the real problems. On the one hand it is quite clear that a legislation without selfregulatory and technical satsifactory solutions will only serve as window dressing but on the other hand without a legislation or without the fear of a legislation (in that context, the PIC's development as a way to avoid the american Decency Act is a good example), it is quite unclear that selfregulatory solutions will be imagined and adopted and that their content will be adequate to ensure privacy protection.

We should like to stress the State's vital obligation to intervene at a time when, in our opinion, deserting the Internet and withdrawing the field of regulation to such a point that it is no longer even decides the general framework, would notally put at risk public order, fundamental liberties and other basic values.

19. The role of the State vis a vis the development of the technical standards and in general of the selfregulation is of crucial importance. Through specific legislation, the government has to encourage the development of technical tools complying with privacy requirements (e.g. In Belgium, we are thinking about a legislation granting certain legal advantages to web sites voluntary accredited). Furthermore, the government might provide research funds in order to develop the needed technical tools and decide to implement for its own notally in the relationships between administration and citizens) the fair information practices and privacy enhancing technologies, he has contributed to develop.

20. Finally and overall, the government has to ensure a better awareness among the citizens about the privacy risk of Internet and the adeqaute solutions the technical tools and the interactivity of the network provide. It is quite clear that the internet's user is himself his own better identity protector. He might decide to prevent the arrival of cookies, to erase them or block their sending; he might through techniques of encryption of anonymisation protect the confidentiality of his message or its anonymity; he might reveal or not certain data, decide to communicate only with rated websites and use his access right to control their activities.

21. In view of these perspectives, our ECLIP project would have to

- evaluate to what extent, presently the websites are effectively aware of the privacy concerns and take into account the D.P. principles in the definition of their practices;
- analyse the practical significance of the DP provisions of the directive in the context of e. commerce (see, supra n° 9 et s.) and suggest to the commission and legislators (see supra n° 11) possible new principles or complementary provisions;
- assess notally through comparative evaluation's grid, the different self regulatory solutions in regard with the D.P. requirements taking into account the three criteria presented above (n° 14 et s.) ;
- provide a list of "adequate" web sites practices after having examined their adequacy with D.P. authorities and checked their practicability with Web site responsibles;
- disseminate vade mecum both to web user to assist them in their evaluation of their privacy risks and possible offered solutions and to web sites controllers propose "fair information practices" in regard with privacy concerns and to assist them to evaluate the quality of the proposed self regulatory mechanisms.