14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

New Privacy Concerns: ISPs, Crime prevention, and Consumers' Rights

By Yaman Akdeniz, Director of Cyber-Rights & Cyber-Liberties (UK)

Abstract:

In November 1998, Cyber-Rights & Cyber-Liberties (UK) developed a "privacy letter" to be sent from a subscriber to an ISP addressing concerns over privacy of communications through a UK ISP. The letter was drafted from the consumers' perspective and raises important issues in relation to ISP privacy policies. The privacy letter was partly developed as a response to the Association of Chief Police Officers ("ACPO"), the Internet Service Providers and the Government Forum's initiatives in relation to developing "good practice guidelines" between Law Enforcement Agencies and the Internet Service Providers Industry. These guidelines describe what information can lawfully and reasonably be provided to Law Enforcement Agencies, under what circumstances such information can be provided, and the procedures to be followed in such cases.

The process initiated by the ACPO Forum has so far excluded the views of concerned citizens and civil liberties organisations. This paper will provide an insight into the activities of the ACPO/ISPs/Government Forum and will argue that procedures can only be properly designed within a legal context which takes due account of individual rights and liberties.

The Paper

With the rapid growth of the Internet as the newest medium for our correspondence, comes the need to review the interaction of conflicting demands for respect for privacy, freedom of expression and the detection and punishment of crime. Although the advancement of technology means that "privacy rights" are more and more in danger and open to abuse, the Internet does not create new privacy issues. Rather, it makes the existing ones - like confidentiality, authentication and integrity of the personal information and correspondence circulated - difficult to control and secure.

There are major concerns about the vehicle the Internet provides for personal snooping not only by commercial institutions but also (and more seriously) by governmental organisations and law enforcement bodies. This working paper deals with the current state of UK Internet Service Providers privacy policies.

In November 1998, Cyber-Rights & Cyber-Liberties (UK) developed a "privacy letter" (see Appendix I) to be sent from a subscriber to an ISP addressing concerns over privacy of communications through a UK ISP. The letter has been drafted from the consumers' perspective and raises important issues in relation to ISP privacy policies.

The privacy letter was partly developed as a response to the Association of Chief Police Officers, the

Internet Service Providers and the Government Forum's initiatives in relation to developing "good practice guidelines" between Law Enforcement Agencies and the Internet Service Providers Industry. These describe what information can lawfully and reasonably be provided to Law Enforcement Agencies, and under what circumstances such information can be provided, and the procedures to be followed in such cases.

Given the concern over cyber-crimes and cyber-criminals it is entirely understandable that the police and the ISPs should wish to develop mutual understanding and support, and to establish working relationships. However, the Forum has so far produced no documents in relation to its meetings. The Forum's membership is also unclear. It includes partial representation through ISPA and LINX to the ISP industry together with several Home Office representatives and ACPO representatives but little is known publicly about its members and its activities apart from the overall aim of the Forum as described above.

Moreover, the views of civil liberties organisations and, more importantly, the views of the users have been excluded from the Forum as no such representation is provided within the Forum: it is partly as a result of this exclusion that the Forum's initiatives and work, if unchecked, could lead to extensive infringements of the rights of individual Internet users and consumers within in the UK.

In an attempt to draw public attention to this issue, Cyber-Rights & Cyber-Liberties (UK) drafted the "privacy letter" (see appendix I) which states that, "it should be the duty of the Internet Service Providers to safeguard the fundamental rights and freedoms of the Internet users to private communications, and in particular their right to privacy with respect to the processing of personal data which is explicitly protected by international agreements such as the European Convention on Human Rights."

To date the work of the Forum seems to have been focused on developing and harmonising a form of request for information by the police to an ISP. The form, which might seem to some addressees to have the appearance of a warrant, is designed to satisfy the ISP that in the circumstances of the particular case the ISP is not prevented by the restrictions in the Data Protection Act 1984 from providing information to the police. Despite its appearance, the form and its associated "good practice guidelines", has no legal basis for imposing any obligation on an ISP to provide any form of disclosure to the police. However, there is a real risk of ISPs being misled by such a form and one purpose of the "privacy letter" is to draw attention to such risks. We are also concerned that the Forum completely neglects the matter of the protection granted by the law to the safeguarding of confidential information.

The privacy letter also aimed to bring the recently enacted Human Rights Act 1998 to the attention of the ISPs. The 1998 Act incorporates the European Convention on Human Rights into UK law and will provide a further ground for action against infringement of privacy rights. We believed at the time, and still believe, that the use of the privacy letter by the consumers would be an important contribution to the whole process by covering the consumers' angle. The publication of the results could bring a more balanced approach and openness to a process that has been secretive and therefore faced with suspicion. The approach we have taken with the development of the "privacy letter" is consistent with February 1999 Recommendation of the Council of Europe "for the Protection of Privacy on the Internet." (see Council of Europe Recommendation (No R (99) 5 of the Committee of Ministers to Member States, at http://www.coe.fr/cm/ta/rec/1999/99r5.htm) The Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways were adopted by the Committee of Ministers on 23 February 1999. According to the Council of Europe Recommendation, these guidelines may be incorporated in or annexed to codes of conduct. The guidelines set out principles of fair privacy practice for both Internet users and ISPs.

As far as the users are concerned, the Council of Europe guidelines recommends that:

> "Your ISP is responsible for proper use of data. Ask your ISP what data he/she collects, processes and stores, in what way and for what purpose. Repeat this request from time to time. Insist that your ISP change them if they are wrong or delete them if they are excessive, out of date or no longer required. Ask the ISP to notify this modification to other parties to whom he or she has communicated your data." (paragraph 10)

The above recommendation is very much in line with our "privacy letter" produced some three months earlier. Furthermore, the guidelines for users state that:

> "If you are not satisfied with the way your current ISP collects, uses, stores or communicates data, and he or she refuses to change his or her ways, then consider moving to another ISP. If you believe that your ISP does not comply with data protection rules, you can inform the competent authorities or take legal action." (paragraph 11)

The Council of Europe requires and encourages Internet users to be concerned about privacy matters and take the necessary action in relation to their online privacy.

One of the questions we asked within the "privacy letter" was whether the ISPs have a privacy policy on such requests from the law enforcement agencies and whether the proposed ACPO good practice guidelines will affect their current policy. Another question, which is of a technical nature, asks what sort of monitoring or backup systems are used by the ISPs and for how long they keep personal data. The letter also asks whether they are capable of actively monitoring all IP traffic from a particular user and if this is done for what purposes.

We have defined "personal data" for the purposes of this letter as follows:

> all traffic data and related information including the following: "the content, origin, destination and timing of my electronic mail messages (sent and received), including the details of any newsgroups to which I subscribe and the details of messages received from or posted to them. Moreover, information about web sites visited, FTP activities and IRC usage by myself or any members of my family through my account through the connection you provide and details of login and connection times."

The privacy letter therefore asks six legitimate questions which in our view should be answered by all ISPs in this country. This view does not derive from any press coverage, and the idea behind the whole concept of developing such a "privacy letter" for the consumers usage is not the creation of a "poison pen campaign", or to create distrust between the Internet users (see further appendices II and III) and their ISPs within the UK. Furthermore, the above mentioned Council of Europe guidelines for the ISPs states that (paragraph 11 of part III) ISPs are responsible for proper use of data.

> "On your introductory page highlight a clear statement about your privacy policy. This statement should be hyperlinked to a detailed explanation of your privacy practice. Before the user starts using services, when he or she visits your site, and whenever he or she asks, tell him or her who you are, what data you collect, process and store, in what way, for what purpose and for how long you keep them. If necessary, ask for his or her consent. At the request of the person concerned, correct inaccurate data immediately and delete them if they are excessive, out of date or no longer required and stop the processing carried out if the user objects to it. Notify the third parties to whom you have communicated the data of any modification. Avoid the hidden collection of data."

Consistent with the Council of Europe approach, the "privacy letter" will remain as a tool that can be used by concerned Internet users to find more about the privacy policies of their ISPs. After all, consumers have a legitimate interest and right to know about the policies of their ISPs. We intend to

publish the responses provided by the UK ISPs but we have no intention to expose those that remain silent, or those that have provided responses in confidence even though we believe that those responses are in the public interest. However, the "privacy letter" has not yet generated many responses from ISPs even though we are aware that many concerned UK Internet users did use the letter, and even though UK ISPs were aware of the existence of this letter through their trade organisations (see appendices II and III), through users, and through the media coverage. Many users informed us that they had considered changing their ISPs but lack of privacy policies or lack of communication from the ISPs or their trade organisations meant that the UK users did not have a possibility to make an informed judgment.

This lack of response on the part of ISPs prompted Cyber-Rights & Cyber-Liberties (UK) to publish a controversial report entitled "Who Watches the Watchmen: Part III - ISP Capabilities for the Provision of Personal Information to the Police," (see http://www.cyber-rights.org/privacy/watchmen-iii.htm). The report follows the discovery by Cyber-Rights & Cyber-Liberties (UK) of a secret briefing (or private as the involved parties claim) to the Association of Chief Police Officers about the ISP industry capabilities for the provision of information to the police about their customers. In a press release CR&CL(UK) stated that "with all these possibilities and capabilities for the provisions of information through the ISPs to the police, the ISPA runs the risk of becoming the Big Brother Providers Association. The leaked report shows that our concerns were fully justified, and that secrecy, rather than 'media disinformation' was at work with the activities of the ACPO/ISPs Forum."

Procedures can only be properly designed within a legal context and we are concerned to ensure that the legal context takes due account of individual rights and liberties. Such procedures are a matter of legitimate public interest, especially to users of the services of ISPs. The discussions of the industry and the law enforcement bodies should have been public, and users' interests should have been represented. Even the ISPs have limited representation, since we understand that ISPA and LINX do not represent the whole of the ISP industry within the UK. This reinforces the need for public awareness.

Transparency, openness and accountability are important features of a healthy society. We believe it is now time for the Government, through Parliament, to intervene in the activities of the ACPO/ISPs, Government Forum and clarify these matters including the laws in relation to interception of communications and the relevant procedures. (see also the Cyber-Rights & Cyber-Liberties (UK) Memorandum to the House of Commons Trade and Industry Select Committee on Electronic Commerce Inquiry, February 1999, at http://www.cyber-rights.org/reports/crcl-hc.htm)

What is healthy for a nation asks David Brin in *The Transparent Society*. (Brin, D., *The Transparent Society, Will Technology Force Us to Choose Between Privacy and Freedom?* Reading: Addison Wesley Longman, 1998, p 119) The answer Brin gives is "accountability". "Many minds and talents working to solve problems through a market of ideas. Since no single ruler can ever spot all errors, especially his own, open criticism helps a nation evade disasters." Therefore, those who are in a position to discuss and influence Internet policy making process, should face public criticism and in the words of Brin, they should even "encourage all the criticism [they] can get". Without such discourse and accountability, there will never be a transparent Society.

A response to these calls for openness and transparency came from one of the ISP trade organisations, the London Internet Exchange ("LINX"). LINX invited industry representatives, public interest groups and the DTI to discuss privacy on the Internet within a new Privacy Forum in March 1999.The proposed first objective of this group of people will be to work together on producing an "Internet Privacy Code" that ISPs would be willing to commit to and this initiative is also supported by ISPA.

This is an important step in the right direction and Cyber-Rights & Cyber-Liberties (UK) will be

involved with these meetings. It is encouraging to see the industry finally responding positively to the consumers' concerns on Internet privacy. The development of an Internet Privacy Code which takes into account users concerns at a national level will be a major step towards the recognition and protection of such rights and values.

Bibliography

See further Akdeniz, Y, & Bohm, N, "Internet Privacy: New Concerns about Cyber-Crime and the Rule of Law," forthcoming in *IT & Communications Law Reports Newsletter*, 1999.

Cyber-Rights & Cyber-Liberties (UK) is at http://www.cyber-rights.org

See also the Cyber-Rights & Cyber-Liberties (UK) Memorandum to the House of Commons Trade and Industry Select Committee on Electronic Commerce Inquiry, February 1999 at http://www.cyber-rights.org/reports/

Appendix I

Cyber-Rights & Cyber-Liberties (UK) Privacy Letter

This letter drafted by Yaman Akdeniz and Nicholas Bohm has b een finalised following extensive discussion within the cyber-rights-UK Mailing List in November 1998. This letter is also available at <http://www.cyber-rights.org/privacy/letter.htm>

Date:

Dear Sirs,

I have had an Internet account with you since [INSERT DATE - TO BE FILLED BY THE USER], and I am writing to raise a concern with you about the confidentiality of Internet communications and Internet users data.

I have read of proposed "good practice guidelines" (formerly known as a memorandum of understanding) between UK Internet Service Providers and the Association of Chief Police Officers (see for example, "Police tighten the Net," *The Guardian*, Online Section, 17 September, 1998 and "Personal privacy versus crime fighting on the electronic frontier," *Computing*, 07 October 1998). This is apparently designed to enable ISPs to be released in certain circumstances from the restrictions on disclosure of personal data imposed by the UK Data Protection laws. My understanding is that the proposed guidelines follow from the initiatives of a recently formed body, "The Association of Chief Police Officers, Internet Service Providers & Government Forum", which held three seminars during October 1998 entitled "Policing the Internet: Working together to address issues and allay concerns".

I wanted to let you, my Internet Service Provider, know that I regard all traffic data and related information as confidential including the following:

"the content, origin, destination and timing of my electronic mail messages (sent and received), including the details of any newsgroups to which I subscribe and the details of messages received from or posted to them. Moreover, information about websites visited, FTP activities and IRC usage by myself or any members of my family through my account through the connection you provide and details of login and connection times."

[THE NEXT SENTENCE WOULD DEPEND ON THE USERS CIRCUMSTANCES, e.g. anyone who communicates with a lawyer by email, or may do so, can reasonably include the following

sentence]

I should also mention that a number of the messages sent and received are not only confidential but are also potentially the subject of legal professional privilege.

Therefore, I would regard the release of the information I have described as a serious breach of confidence and actionable as such and also in contract and also, where applicable, under the Data Protection Act 1984. Short of what is judicially authorised, I have the strongest objection to private bargains being made for the release of confidential information (whether under the so called "good practice guidelines" or otherwise). Such guidelines have no legal force under current UK law, and as my Internet Service Provider, you are not bound to provide any sort of information if you are not provided with judicial authority.

In fact, it should be your duty to safeguard my right to private communications, which is explicitly protected by international agreements such as the European Convention on Human Rights. Please also note that the recently enacted Human Rights Act 1998 incorporates the European Convention on Human Rights into UK law and will provide a further ground for action against infringement of my privacy rights.

To clear any doubts about the excellent services that you provide, I would like you to answer the following specific questions related to the content of this letter:

(1) Does your organisation take part in the Association of Chief Police Officers, Internet Service Providers & Government Forum or has it been aware of such discussions ?

(2) Has your organisation been approached by the above forum to take part into such discussions and what has been the response ?

(3) What is your organisation's policy on such requests from the law enforcement agencies? If there is a written policy, please let me have a copy. Will the proposed good practice guidelines (previously known as the Memorandum of Understanding) affect your current policy ?

(4) What sort of monitoring or backup systems are used and for how long do you keep personal data (as explained above) ? Is [insert name of the ISP] capable of actively monitoring all IP traffic from a particular user and if this is done for what purposes ?

(5) Are you registered with the Data Protection Registrar, and if so for what purposes can you disclose data and to whom ?

(6) Do you have any objection to publication of your replies? If so, please give the reasons for your objection.

I very much hope that you will be able to confirm that you will respect the confidentiality of the information I have described.

[PLEASE FEEL FREE TO MODIFY OR DELETE THE FOLLOWING PARAGRAPH]

I have a high regard for the quality of your service, especially your user support, and have recommended you to others who have been equally pleased with the results. I hope that your approach to customer confidentiality will be just as commendable and I hope to hear from you soon.

Yours faithfully,

Appendix II

The ACPO/ISPs, Government Forum Response to the CR&CL(UK) Privacy letter

Yaman Akdeniz

c/o Centre For Criminal Justice Studies,

University of Leeds,

Leeds LS2 9JT,

UK

By email

2nd December 1998

Dear Sir,

I am writing in response to your letter as published at www.cyber-rights.org/privacy/letter.htm. I am the currently nominated ISP press spokesperson for the ACPO/ISP meetings.

Your letter and your letter writing campaign seems to be based on inaccurate press articles, allow me to put the record straight –

1. ACPO and industry representatives have been discussing a procedure through which police requests for information will be made to ISPs.

2. This work is not concluded yet.

3. The information that might be released by this procedure is not intended to be the contents of emails or messages despite what you read in the press.

4. The main purpose of the procedure is to uphold the privacy of individuals by seeking to ensure that data is not requested or released except in accordance with the specific provisions of the Data Protection Act that allow for that release.

5. The completion of the relevant form by law enforcement agencies will be a necessary but not sufficient condition for the release of information. In other words there will still be occasions where ISPs may refuse to release information unless and until they are presented with a warrant or court order.

In short this procedure is to ensure that 50 odd police forces and 200+ ISPs and the individuals that work for them remain within the law, the complete opposite of the implication in the second paragraph of your letter.

It seems to me, from talking to the many journalists that have phoned me recently, that the misinformation about this matter may be being spread deliberately and I thank you for your opportunity to clear the matter up. I trust you will now cease your letter writing campaign.

There are some very real issues about how the law relating to the use of the Internet should develop, exactly what legal protection emails or other information should have is clearly part of this debate. Do not confuse your legitimate concerns over these issues with ISPs and policemen and women trying to carry out their jobs in accordance with the laws that exist today.

Yours Sincerely

Tim Pearson

Member of the Council of ISPA

ps For background information I have attached the terms of reference of the ACPO/ISP/Government forum.

ACPO/ISP/Government Forum

Terms of Reference

Overall Aim:

To develop and maintain a working relationship between the Internet Service Providers Industry and Law Enforcement Agencies in the UK, such that criminal investigations are carried out lawfully, quickly and efficiently while protecting the confidentiality of legitimate communications and with minimum impact on the business of the Industry.

Objective:

To develop good practice guidelines between Law Enforcement Agencies and the Internet Service Providers Industry describing what information can lawfully and reasonably be provided to Law Enforcement Agencies, under what circumstances it can be provided, and the procedures to be followed.

Tasks:

Identify and review the legal requirements to be met to provide the information

Identify the information that can be provided from a technical perspective.

To research and identify areas of legal uncertainty relating to the use of information from the Internet as evidence and to make recommendations to resolve any ambiguities.

Develop an accepted procedure for requesting and providing information

Put in place procedures to pay for resources used

Co-ordinate and demonstrate leadership towards similar activities internationally

Appendix III

CR&CL(UK) Response to the ACPO/ISPs Government Forum response

03 December, 1998

To: Mr. Tim Pearson, Member of the Council of ISPA

ISP press spokesperson for the ACPO/ISP meetings

Dear Mr. Pearson,

Thank you for your letter dated 02 December, 1998 concerning the privacy letter developed by Cyber-Rights & Cyber-Liberties (UK) at http:// www.cyber-rights.org/privacy/letter.htm. We welcome your willingness to respond.

We propose to respond to your points by quoting and commenting on them:

"Your letter and your letter writing campaign seems to be based on inaccurate press articles, allow me to put the record straight."

Our privacy letter asks six legitimate questions which in our view should be answered by all ISPs in this country. This view does not depend on the press coverage, and indeed your reply reinforces our view, for reasons we explain below.

We cannot altogether sympathise with your difficulty in getting accurate press coverage, as this must follow from the undesirable secrecy in which you have tried to conduct your work. Perhaps you should consider holding open meetings in the future and producing full transcripts of all past meetings. Furthermore, procedures can only be properly designed within a legal context and we are concerned to ensure that the legal context takes due account of individual rights and liberties.

"ACPO and industry representatives have been discussing a procedure through which police requests for information will be made to ISPs."

Such procedures are a matter of legitimate public interest, especially to users of the services of ISPs. The discussions should have been public, and users' interests should have been represented. Even the ISPs have limited representation, since we understand that ISPA represents only some 70 out of about 300. This reinforces the need for public awareness.

"This work is not concluded yet."

That is why we are anxious to ensure that there is wider debate now rather than later.

"The information that might be released by this procedure is not intended to be the contents of emails or messages despite what you read in the press."

It is regrettable that you remain unwilling to say what information is within the scope of the procedure you are discussing, and that your form of reply is wholly negative. The public should know what it is that law enforcement is seeking from ISPs.

And as you know from our privacy letter, it is much more than the contents of emails that we say is confidential.

"The main purpose of the procedure is to uphold the privacy of individuals by seeking to ensure that data is not requested or released except in accordance with the specific provisions of the Data Protection Act that allow for that release."

We firmly support your objective of ensuring compliance with Data Protection Law. As your next point acknowledges, that is not by itself enough.

"The completion of the relevant form by law enforcement agencies will be a necessary but not sufficient condition for the release of information. In other words there will still be occasions where ISPs may refuse to release information unless and until they are presented with a warrant or court order."

The procedure you are working on may be sufficient to release an ISP from the prohibitions of the

Data Protection Act. It plainly cannot release the ISP from liability for breach of confidence (nor can it release the law enforcement agency concerned from the risk of liability for interfering with contractual relations between the ISP and its customer by procuring a breach of confidence).

An ISP is in fact generally bound to refuse to release confidential information without judicial authority. There may be a small number of special cases where an ISP is entitled to release otherwise confidential information: these are far from easy for an ISP or the police to identify. If the Forum believes it can define these cases, and can establish a procedure for determining what evidence would justify an ISP in accepting that such a case had been made out, with the Forum's work conducted in an open way, that might be a valuable function. But given the difficulties and risks involved, such a debate might very well conclude that judicial authority was the only proper way to proceed.

In this connection I am sure that the significance of the recent incorporation into domestic UK law of Article 10 of the European Convention on Human Rights cannot have escaped you.

"In short this procedure is to ensure that 50 odd police forces and 200+ ISPs and the individuals that work for them remain within the law, the complete opposite of the implication in the second paragraph of your letter."

The procedure would be more like to achieve that commendable result if it had taken place in public with representation of a wider range of interests. That might have avoided your having entirely overlooked the law of breach of confidence as reinforced by the Human Rights Act 1998.

"It seems to me, from talking to the many journalists that have phoned me recently, that the misinformation about this matter may be being spread deliberately and I thank you for your opportunity to clear the matter up."

We are certainly keen not to spread misinformation, and are glad to publish your letter. The delay since 10th November when we were first in touch with you may have been unavoidable, but it was your delay and not ours.

"I trust you will now cease your letter writing campaign."

Our letter has been published for the use of ISP customers, and it is up to them to decide whether your response has allayed their concerns. Our comments may suggest to you that considerable concerns remain. If ISP customers share that view, they will no doubt continue to press for answers to their letters. If this is a campaign (your choice of word, not ours), it is their campaign.

The letter is not directed against a single ISP or an ISP trade association, or indeed against the ACPO/ISP Forum. It raises important questions that are of legitimate interest to consumers, and consumers have a right to know about the policies of their ISPs.

"There are some very real issues about how the law relating to the use of the Internet should develop, exactly what legal protection emails or other information should have is clearly part of this debate."

We agree: debate it in public. In the absence of such an open debate it is healthy and proper for concerned people to make their points as loudly as possible.

"Do not confuse your legitimate concerns over these issues with ISPs and policemen and women trying to carry out their jobs in accordance with the laws that exist today."

ISPs are of course not trying to do the same job as members of law enforcement agencies, and it

would be very unwise to give the impression that ISPs are being recruited to help do the work of law enforcement. Both groups must stay within the law as they do their important work; important not just to them but to all of us. Attempts to co-operate in secret have risked overlooking important legal issues, and gaining bad publicity which we hope is undeserved.

Thank you for providing the Forum's Terms of reference, a most important document. What is most striking about it is the complete absence of any concept of the accountability of the ISPs to their customers or of the Forum to the public.

In summary we are grateful for your letter, and have found it useful up to a point; but it has carefully not answered any of the questions that we asked in our privacy letter with respect to individual ISP policies. We think those answers are valuable to all concerned, and we intend to publish all responses through our pages together with this letter.

Yours sincerely,

Signed

Mr Yaman Akdeniz, Director

Prof. Clive Walker, Deputy Director

Mr Nicholas Bohm, E-Commerce Policy Adviser

Dr. Brian Gladman, Technology Policy Adviser

Cyber-Rights & Cyber-Liberties (UK) - http://www.cyber-rights.org