Project on Cybercrime
www.coe.int/cybercrime

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France
Version 12 March 2008

(draft)

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

Prepared by
Cormac Callanan (Ireland)
Marco Gercke (Germany)

These draft guidelines are the result of several rounds of discussions with representatives from industry and law enforcement who met between October 2007 and February 2008 under the auspices of the Council of Europe's Project on Cybercrime.

This draft will be further discussed at the conference Cooperation against Cybercrime (Council of Europe, Strasbourg, France) on 1-2 April 2008. It will also be complemented by a detailed background study.

The guidelines will be a non-binding tool that should help law enforcement and service providers in any country around the world organise their cooperation against cybercrime while respecting each others' roles and responsibilities as well as the rights of internet users.

Those unable to participate in this conference are invited to send their comments to **coe-study-comments@aconite.ie**.

Feedback received by 28 March may be fed into the discussions at the conference.

Guidelines (draft) for the cooperation between law enforcement and internet service providers against cybercrime[1]

Introduction

1. Building an information society requires the strengthening of trust in information and communications technologies (ICT's), the protection of data and privacy, and the promotion of a global culture of cyber-security in a context where societies worldwide are increasingly dependent on ICT and thus vulnerable to cybercrime;

2. The First and Second World Summit on the Information Society (Geneva 2003, Tunis 2005) – among other things – committed to build an inclusive information society where everyone can create, access, utilize and share information and knowledge, achieve their potential and improve their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights, and which calls for new forms of partnerships and cooperation among governments, the private sector, civil society and international organisations;

3. Internet service providers (ISP) and law enforcement authorities (LEA) play a crucial role in the realization of this vision;

4. National legislation in line with the Convention on Cybercrime of the Council of Europe (the "Budapest Convention") helps countries create a sound legal basis for public-private cooperation, investigative powers as well as international cooperation;

5. The Convention on Cybercrime in Article 1 defines "service provider" in a broad manner as meaning:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

6. In order to enhance cybersecurity, minimise illegal use of services and build trust in ICT, it is essential that Internet service providers and law enforcement authorities cooperate with each other in an efficient manner with due consideration to their respective roles, the cost of such cooperation and the rights of citizens;

7. The purpose of the present guidelines is to help law enforcement authorities and Internet service providers structure their interactions in relation to cybercrime issues. They are based on existing good practices and should be applicable in any country around the world in accordance with national legislation and respect for the freedom of expression, privacy, the protection of personal data and other fundamental rights of citizens;

8. It is therefore recommended that States, law enforcement authorities and Internet service providers undertake the following measures:

[1] This document does not necessarily reflect official positions of the Council of Europe.

Common guidelines

9. States should adopt regulations in their national law in order to fully implement the procedural provisions of the Convention on Cybercrime and to define investigative authorities and obligations of law enforcement. This will

- ensure efficient work of law enforcement authorities
- protect the ability of Internet service providers to provide services
- ensure that national regulations are in line with global standards
- promote global standards instead of isolated national solutions;

10. Law enforcement authorities and Internet service providers should be encouraged to engage in information and intelligence exchange to strengthen their capacity to identify and combat emerging types of cybercrime. Law enforcement authorities should be encouraged to inform service providers about cybercrime trends;

11. Law enforcement and Internet service providers should promote a culture of cooperation – rather than confrontation - including the sharing of good practices. Service providers should be encouraged to assist law enforcement with education, training and other support on their services and operations, while law enforcement should be encouraged to provide explanations and assistance to service providers regarding non-case-related investigation techniques in order for them to understand how their cooperation will result in more efficient investigations against crime and better protection for citizens. Regular meetings in order to exchange experience and resolve problems are encouraged;

12. Law enforcement and service providers should be encouraged to develop written procedures for cooperation with each other. Both parties should be encouraged to provide structured feedback on the operation of these procedures to each other;

13. Formal partnerships between law enforcement and service providers should be considered in order to establish longer-term relationships with proper guarantees for both sides that the partnership will not infringe any legal rights on the side of the industry or limit any legal powers on the side of law enforcement;

14. Both law enforcement authorities and Internet service providers should protect the fundamental rights of citizens according to United Nations and other applicable European and international standards as well as domestic law. This places reasonable limits to the level of cooperation possible;

15. Both sides should be mindful of the costs involved in creating and responding to requests. Procedures should be developed with consideration of the financial impact;

Measures to be taken by law enforcement

16. Broad and strategic cooperation – Law enforcement should be encouraged to assist service providers by engaging in a broad and strategic cooperation with industry that would include conducting regular technical and legal training seminars, as well as providing feedback on investigations conducted based on complaints filed by service providers or on the intelligence gathered based on known criminal activity reported by the service providers;

17. Procedures for requests – Law enforcement should be encouraged to prepare written procedures for the issuing and processing of requests, and ensure that requests are carried out pursuant to the agreed procedures;

18. Training – Law enforcement should be encouraged to provide training to a designated set of their personnel on how to implement these procedures, including the manner in which records may be obtained from service providers and how to process information received, but also on internet technologies and their impact in general;

19. Technical resources – Law enforcement personnel responsible for cooperation with service providers should be equipped with the necessary technical resources, including internet access, an agency-issued email address that makes the affiliated agency apparent in the address, and other technical resources to permit them to receive information securely from a service provider electronically;

20. Designated personnel and contact points – Interaction between law enforcement and service providers should be limited to trained personnel. Law enforcement should be encouraged to designate contact points for their cooperation with service providers;

21. Authority for requests – Law enforcement authorities should be encouraged to define clearly in their written procedures which law enforcement personnel can authorise what type of measures and requests to Internet service providers and how these requests can be validated/authenticated by Internet service providers;

22. Law enforcement should be encouraged to make information available to Internet service providers on their procedures and, where possible, which personnel or which nominated job positions are responsible for cooperation with Internet service providers;

23. Verification of source of request – The source of a request from law enforcement should be verifiable by service providers:

- All correspondence should include the contact name, telephone number and e-mail address of the law enforcement agent(s) seeking the records so that the service provider can contact the requesting individual if issues arise
- service providers should not be asked to correspond with an agent through the agent's personal e-mail address, but rather through an appropriate agency-provided e-mail account
- all letters should be on department letterhead, and all correspondence should include the agency's main switchboard number and website address so that service providers can take steps to verify the authenticity of requests if deemed appropriate;

24. Written requests – Requests from law enforcement to service providers should be made in writing and leave a documentary trail. In extremely urgent cases, oral requests may be acceptable, but must be immediately followed up by written documentation;

25. Standard request format – At the national level, and if possible internationally, law enforcement should be encouraged to standardise and structure the format used for sending requests and for responding to requests. As a minimum requests should contain the following information:

- Registration number
- Reference to legal basis
- The specific data requested
- Information to verify the source of the request;

26. Specificity and accuracy of requests – Law enforcement should be encouraged to ensure that requests sent are specific, complete and clear, and provide a sufficient level of detail to allow service providers to identify relevant data. They should be encouraged to ensure that requests are sent to the service provider that has the records. Requests for multiple and unspecified data should be avoided;

27. Law enforcement should be encouraged to provide as many facts about the investigation as possible without prejudicing the investigation or any fundamental rights in order to enable service providers to identify relevant data;

28. Prioritisation – Law enforcement should be encouraged to prioritise requests, especially those related to large volumes of data, to enable service providers to address the most important ones first. Prioritization is best done in a consistent manner across national law enforcement authorities and if possible internationally;

29. Appropriateness of requests – Law enforcement should be encouraged to be mindful of the cost that requests entail for service providers and give service providers sufficient response time. They should be mindful that service providers may also need to respond to requests from other law enforcement authorities, and should be encouraged to carefully monitor volumes submitted;

30. Confidentiality of data – Law enforcement should ensure the confidentiality of data received;

31. Avoid unnecessary cost and disruption of business operations – Law enforcement should be encouraged to avoid unnecessary cost and disruption of business operations of the service providers and other types of business;

32. Law enforcement should be encouraged to restrict the use of emergency contact points to extremely urgent cases only to ensure the service is not abused;

33. Law enforcement should be encouraged to ensure that preservation orders and other provisional measures are followed up in a timely manner by disclosure orders, or the Internet service provider is informed in a timely manner that preserved data is no longer required;

34. International requests – For requests addressed to non-domestic Internet service providers, domestic law enforcement authorities should be encouraged to ensure that international requests make use of the Convention on Cybercrime and the network of 24/7 law enforcement points-of-contact for urgent measures, including preservation orders/requests;

35. Requests for International mutual legal assistance – Law enforcement and criminal justice authorities should be encouraged to take the necessary steps to ensure that requests for provisional measures are followed by international procedures for mutual legal assistance;

36. Coordination among law enforcement agencies – law enforcement authorities should be encouraged to coordinate their cooperation with Internet service providers and share good practices among each other nationally and internationally. Internationally they should make use of relevant international representative bodies for that purpose;

37. Criminal compliance programmes – Law enforcement should be encouraged to organise their interactions outlined above with service providers in the form of a comprehensive criminal compliance programme, and provide a description of such programme to service providers, including:

- The information necessary to contact the law enforcement designated criminal compliance personnel, as well as the hours during which such personnel are available
- The information necessary for service provider to be able to provide documents to the criminal compliance personnel

- Other particulars specific to the law enforcement criminal compliance personnel (such as the extent that a law enforcement operates/co-operates in multiple countries, documents to be translated into a particular language etc.);

38. Audit of the compliance system – Law enforcement authorities should be encouraged to track and audit the system of processing requests for statistical purposes, for identifying strengths and weaknesses and publish such results if appropriate;

Measures to be taken by service providers

39. Cooperation to minimize illegal use of services – Subject to applicable privacy and other laws, as well as user agreements, service providers should be encouraged to cooperate with law enforcement to help minimize the extent to which services are used for fraudulent or other criminal activity;

40. Service providers should be encouraged to report known criminal incidents affecting the Internet service provider to law enforcement;

41. Follow up to requests from law enforcement authorities – Service providers should be encouraged to undertake all reasonable efforts to assist law enforcement and track data requested;

42. Procedures for responding to requests – Service providers should be encouraged to prepare written procedures for the processing of requests, and ensure that requests are followed up to pursuant to the agreed procedures;

43. Training - Service providers should be encouraged to make sure that sufficient training is provided to those responsible for implementing these procedures;

44. Designed personnel and contact points – Service providers should be encouraged to designate trained personnel as contact points for cooperation with law enforcement;

45. Emergency assistance – Service providers should consider establishing a means by which law enforcement may reach their criminal compliance personnel outside of normal business hours to address emergency situations. Service providers should be encouraged to provide law enforcement with relevant information such as contact information and conditions for emergency assistance;

46. Resources – Service providers should be encouraged to provide contact points or personnel responsible for cooperation with law enforcement with the resources necessary to enable them to comply with requests from law enforcement;

47. Criminal compliance programmes – Service providers should be encouraged to organise their cooperation with law enforcement in the form of comprehensive criminal compliance programmes, and provide a description of such programmes to law enforcement, including:

- The information necessary to contact the providers' designated criminal compliance personnel, as well as the hours during which such personnel are available
- The information necessary for law enforcement to be able to provide documents to the criminal compliance personnel
- Other particulars specific to the providers' criminal compliance personnel (such as the extent that a service provider operates in multiple countries, documents to be translated into a particular language etc.);

48. Verification of source of requests – Service providers should be encouraged to take steps to verify the authenticity of requests received from law enforcement to the extent possible and necessary to ensure that customer records are not disclosed to unauthorized personnel;

49. Written response – Service providers should be encouraged to respond to requests from law enforcement in writing and ensure that a documentary trail is available;

50. Standard response format – Taking into account the format for requests used by law enforcement, service providers should be encouraged to standardise the format for sending information to law enforcement;

51. Service providers should be encouraged to process requests in a timely manner, in line with the written procedures they have defined and provide guidelines to law enforcement on the average delays incurred to respond to requests;

52. Validation of information sent – Service providers should be encouraged to ensure that information transmitted to law enforcement is complete, accurate and protected;

53. Confidentiality of requests – Service providers should ensure the confidentiality of requests received;

54. Explanation for information not provided – Service providers should be encouraged to provide explanations to the law enforcement authority sending a request if requests are rejected or information cannot be provided;

55. Information about services offered – In order to allow law enforcement to make specific and appropriate requests, service providers should be encouraged to provide information on the type of services offered, including web links to the services and additional information as well as contact details for further information;

56. Where possible, the Internet service provider should be encouraged to provide a list of which types of data could be made available for each service to law enforcement on receipt of a valid disclosure request from law enforcement accepting that not all this data will be available for every criminal investigation;

57. Audit of the compliance system – Service providers should be encouraged to track and audit the system of processing requests for statistical purposes, for identifying strengths and weaknesses and publish such results if appropriate;

58. Coordination among service providers – being mindful of anti-trust/competition regulations service providers should be encouraged to coordinate their cooperation with law enforcement and share good practices among each other, and make use of service provider associations for that purpose.