Legal Aspects of Open Public Networks

Adam Burns, Network Commons, free2air,

Bruce M. Simpson, BSD Developer, Consume advocate,

.nbco

Contents

Introduction

1. This document is intended to provide a guide to open public network node-holders, and administrators of those nodes, of the legal implications for open public networks and of holding nodes and administrating them. There has been much said on various lists and sites about the impact of various pieces of legislation, and the legal liability that will follow. In our opinion, some of this advice is wrong, in many respects.

2. Our intention therefore is to provide a complete guide of those liabilities, both criminal and civil, to node-holders and admins. We are of the view that other areas of law will impact

on open public networks. This is of course a working document. Anyone who is of the view that an aspect of the legal analysis is wrong and/or outdated is strongly encouraged to contact the authors with their views at info@networkcommons.org . Additionally if individuals consider that a further area or areas need to be covered, please contact us and we will update or incorporate your ideas.

3. Please note that this document is not intended to provide a best practice guide; the practices which you choose to adopt are of course a matter for you, legal or illegal; this document merely aims to inform individuals as to their liabilities, so that they can make informed choices as to the practices they want to adopt and why. We are not able to provide any kind of risk analysis of the various approaches that can be adopted; this is simply because there have been very few, if any, test cases in this area.

4. This document can and should be copied and distributed as you see fit. However we would ask that if changes are made to this document, we should be informed about them at the above address so we can incorporate and/or research and/or otherwise discuss these ideas.

5. The law applies to England, Northern Ireland and Wales it is stated as at **02 June 2004.**

Definitions and Scope

6. An “open public network”, as defined within this document, is a computer network consisting of a node (also known as a gateway), residing behind the Network Termination Point with the Public Switched Telephone Network, through which it has wired connectivity to the Internet at large. In turn, this node may have wired or wireless connectivity to several clients, which is unrestricted in nature, that is, the clients are not distinguished between based on MAC address or other identifying information.

7. A “node-holder” is defined to be the party who hosts a node within an “open public network” on their premises. The “node-holder” may or may not own the physical hardware but is responsible for the node's physical situation and location.

8. A “sys-ad” is an abbreviation of “systems administrator”, defined to be the party who administers a node and is responsible for its ongoing operation and correct network function.

9. Both the roles of “node-holder” and “sys-ad” may be assumed by several different individuals or the same individual. A “sys-ad” may administer a single node, or potentially multiple nodes, within an “open public network”.

10. It is important to note that the networks referred to above whether wireless or wired are those networks that start at the telephone socket, i.e. the Network Termination Point. Different legal aspects apply to information being transferred across the Public Switched Telephone Network.

11. This analysis is intended solely for those individuals and groups who are allowing other individuals to share their resources for free. As soon as charges are made for use of those resources, then different considerations apply. This is particularly so in relation to providing a service, albeit not as an ISP and is outside the scope of this document. Further, it should be noted that we are unlikely in the future, to include a section in this document considering the legal implications relating to the paid sharing of resources (particularly bandwidth), as we are of the view that if you wish to make money out of this, then go and pay a fucking lawyer with your profits.

12. Additionally, this document does not cover networks which are provided by employers for use by their employees, the law in relation to vicarious liability and defamation is entirely different, and you will be dangerously misled if you rely on this document in such a situation.

Terms and Conditions and Acceptable Use Policies

13. Some, but not all ISPs, restrict broadband sharing. There are various mechanisms that certain ISPs have used to restrict sharing, for example, restricting the broadband access to one computer only (restriction to a single MAC address is common practice for many cable providers), or members of the same "household" or premises, etc. Use of your broadband connection for an open public network, i.e. bandwidth sharing, may conflict with either the Terms and Conditions and/or Acceptable Use Policies of your ISP.

14. Firstly, we recommend checking the terms and conditions **AND** acceptable use policy of your ISP before you sign up with

their service. It is often very difficult to find these documents on the service providers website, but persevere and read them. Find out if the ISP expressly restricts bandwidth sharing; if not, feel free to sign up. Note that there are lists of ISPs which do not restrict sharing on the web, and it may be easier to select one of these as a prospective ISP.

15. However, if the potential ISP does not permit bandwidth sharing, we recommend amending the terms and conditions before you sign up, or asking them to permit you to do so. If you receive no response provide a deeming provision so that your amendments will be incorporated. Make sure that you keep copies of your communications with the ISP, and your amendments to their terms and conditions, in a safe place.

16. Although such amendments have been made by some individuals, and we know of no ISP rejecting them as yet, we do not have any experience of an ISP trying to prevent or restrict bandwidth sharing. It is likely that if you fall foul of their terms and conditions they will simply cut off your service, but it would be open to them to sue you for breach of contract.

17. We would be extremely interested to hear of anyone who has had problems with their ISP in this respect and would urge anyone with such a problem or experience to contact us. Further, if you do have such a problem, do contact us and we may be able to provide advice and support.

Terms and Conditions Summary

18. Make sure or make your ISP accept bandwidth sharing.

Privacy

The Insatiably Curious Sys-ad

19. When providing open public networks various different hardware and/or operating system configurations can be used. By way of example, if bandwidth is being shared over a wireless network using commercial off-the-shelf hardware such as a Draytek, Cisco or Linksys wireless router and a Windows system, the information available to the node-holder/sys-ad of that node, as to the use the wireless network users are putting the network to, is severely circumscribed. The node-holder/sys-ad is unlikely to be able to gain much more information than the MAC address of the wireless network user, the name of the wireless client machine, and its network speed.

    The key point here is that additional hardware and software would be needed to obtain further information, **in addition to the node itself;** for example, a wireless card capable of 'monitor mode', a packet sniffer such as Ethereal, and/or a wireless network auditing tool such as Kismet. These tools can provide information such as surfing habits, sites visited, e-mail addresses, and complete transcripts of e-mail contents.

    By way of contrast, if an open public network is being provided using open-source tools, the node-holder/sys-ad potentially has direct control over the means of inter-networking. The information provided by the tools described above could potentially be obtained directly from the node itself. In these circumstances, the legal exposure of individuals who chose to run their networks in this way is likely to be much higher.

20. The insatiably curious sys-ad may well have data on their systems which they have chosen to view from their network users, which will infringe both the criminal law (see below in relation to child pseudo-pornography), and additionally

infringe the network users rights to privacy. In these circumstances the sys-ad may well be directly exposing themselves to criminal and civil liability for these infringements.

21. A node-holder/sys-ad will need to consider the Data Protection Act 1998, and whether the data they hold renders the node-holder/sys-ad in breach of the Act, and whether that node-holder/sys-ad should be registered under the Act.

The Data Protection Act 1998

22. The Data Protection Act 1998 is intended to provide individuals access to "personal data" held about them by certain bodies who are "data controllers" under the Act. Firstly then a node-holder/sys-ad must consider whether they hold "personal data" of their network users; if they do, then they should next consider whether they are "data controllers" as defined under the Act.

23. A great deal of help as to the Act and its ambit is provided on the Information Commissioner's website; see http://www.informationcommissioner.gov.uk/eventual.aspx

24. Personal data, is defined under section 1 of the Act as follows:

> "personal data" means data which relate to a living individual who can be identified-
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
>
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

25. It is possible that node-holders/sys-ads will have access to "personal data" as defined under the Act. E-mail addresses are considered to be personal data, see: http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Protection%20of%20Privacy%20on%20the%20Internet.pdf

Indeed it is likely that other data which is in possession of the node-holders/sys-ads, such as a home address, will render the individual identifiable, and therefore such data will fall within the definition of "personal data" under the Act.

26. Clearly, if the node-holder/sys-ad holds only the MAC address and/or network speed and/or computer name of the network user(s), then such data cannot be considered to be "personal data" under the Act, as it would be impossible to identify an individual from that data alone. Furthermore, if someone has knowledge that a certain MAC address belongs to say JaneHSmith, that will not render such information "personal data" as to become "personal data"; it must be recorded on a computer (or a paper filing system) under section 1 of the Act. However, if the MAC address on the system is labelled on the system itself, for example, as JaneHSmith's computer, then this may be sufficient to render it "personal data" under the Act.

27. Next, the node-holder/sys-ad will need to consider the purposes for which the data is held. The Data Protection Act, provides protection for data which is held other than for domestic purposes (in accordance with section 36 of the Act). A node-holder/sys-ad is likely to hold data other than for domestic purposes; in this case, they are likely to be covered by the Act.

28. A “data controller” is an individual, company or organisation, that decides why personal data is held, and the way such information is dealt with, as per section 1 of the Act. “Data controllers” hold two obligations in relation to the personal information they hold, namely, to comply with the 8 principles of good data protection principles (Set out in Part I of Schedule 1 of the Act), and to register themselves with the Information Commissioner, in accordance with section 16 of the Act. Further, it worth noting that complying with the 8 principles of good data protection or registering under the Act is neither difficult, onerous or particularly expensive.

29. The Information Commissioner's website provides some very useful documents, which provide further guidance on these points: http://www.informationcommissioner.gov.uk/eventual.aspx?id=1162

Data Protection Summary

30. It is likely that at least some node- holders/sys- ads have data which is subject to protection under the Data Protection Act. The above analysis is merely to identify whether, you in fact, hold such data. If you are a node- holder/sys- ad who does hold personal data (as defined under the Act) on your computer, you will have to consider your obligations under the Act, and additionally, which information you should give to your network users. Failure to register as a data controller with the Information Commissioner is a criminal offence.

31. This document does not describe the procedure for registration (the Information Commissioner refers to this process as notification), the information you have to provide

to your network users, or indeed the 8 principles of good data management as described under the Act. For further guidance, the best resource to consult is the Information Commissioner's Website, as referenced above.

32. It is clear from the above analysis, that deliberately limiting the data that a node- holder/sys- ad holds from the network users will therefore render registration/notification and compliance with the Act unnecessary. This is of course, because you will hold no "personal data" which you have to protect.

The Regulation of Investigatory Powers Act 2000 and Associated Statutes

33. Regulation of Investigative Powers Act 2000 (RIP) provides the statutory authority for the State to monitor citizens' communications. The Act has caused much controversy; in summary, individuals and campaigning groups have raised concerns as to the far reaching powers of the State under this Act. Criticism has been made on the basis that it infringes individual rights to privacy and freedom of speech. This document does not consider the pros and cons of the statutory framework, we merely consider the application of the Act to open public networks.

34. RIP provides, as far as relevant in **Section 1**

"1 (1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of—

(a) a public postal service; or

(b) a public telecommunication system.

(2) It shall be an offence for a person—

(a) intentionally and without lawful authority, and

(b) otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection,

to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system.

35. Section 1 ensures that an individual's communications cannot be intercepted across public or private networks intentionally and without lawful authority, save as excluded by subsection (6) which allows an individual with a right to control the operation or the use of a private system; or who has the express or implied consent of such a person to make the interception. In effect, this means that over private networks there can be no interception of communications save by the individual with the right to control the network or with the consent of both the sender and receiver of the communication.

36. Section 1 is intended to enshrine the right of the citizen to privacy of electronic communication (and postal communications). As can be seen a distinction is made between public and private telecommunications systems.

37. In the authors' opinion, this is an extremely poorly drafted and confusing piece of legislation. The Act attempts to distinguish between what is a public or private telecommunications system as follows:

> Section 2 (1) of the Act provides —
>
> > "private telecommunication system" means any telecommunication system which, without itself being a public telecommunication system, is a system in relation to which the following conditions are satisfied—
> >
> > (a) it is attached, directly or indirectly and whether or not for the purposes of the communication in question, to a public telecommunication system; and
> >
> > (b) there is apparatus comprised in the system which is both located in the United Kingdom and used (with or without other apparatus) for making the attachment to the public telecommunication system;

38. Section 2(1) defines a public and private system as follows, a public telecommunications system means any such parts of a telecommunication system by means of which any public telecommunications service is provided as are located in the United Kingdom. So what, then, constitutes a "public telecommunications service"? This is defined to be any

telecommunications service which is offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom. It seems clear from the intention of the Act that the term "public telecommunication service" refers to ISPs, Mobile phone companies and so on, i.e. companies which provide services to a substantial section of the public or the public at large. Private Telecommunication Systems would refer to corporate network or college networks. Considering the intention of the Act, it would appear that open public networks would be a "private telecommunication system", but since access is offered to the public at large, and the definition of Public Communications Service is so poorly drafted, it is arguable that open public networks would fall within the definition of "public communications service". In the authors' view, this demonstrates the difficulties inherent in the Act. Currently, there is no further guidance as to this point.

39. At this point the distinction between public and private is not of great significance. RIP authorises the State, under specified circumstances, to issue warrants requiring individuals to allow interception of communications over their network. Failure to comply or tipping off the individuals concerned is an offence.

40. However, the distinction between public and private telecommunications services is compounded by the Anti-Terrorism, Crime and Security Act 2001 which the State is using to encourage (and if they cannot be encouraged to require) those companies that provide telephone and communication systems to keep " communications data" for long periods just in case that information might be helpful in the investigation of criminal offences. Unhappily, communications provider means a person who provides a postal service or a telecommunications service, this Act does

not distinguish between a private or public telecommunications service, therefore in theory it applies to open public networks. A voluntary Code of Practice has been introduced, to encourage communications providers to voluntarily retain data, this has caused a great deal of anger within the ISP community see http://www.out-law.com/php/page.php?page_id=dataretentionisps1063885491&area=news. It is worth noting that this is only a voluntary code of practice and so does not require compliance. In the authors' view, once more, it was not Parliament's intention to apply such legislation to such things as open public networks, but, due to the poor drafting, it is a least arguable that the Code of Practice will apply. This is of no real significance currently, as the Code of Practice is only voluntary. However, it is suggested that it would be in the interests of open public network communities to become involved in any further consultations to attempt to exclude themselves from the definition of communications provider.

41. Clearly, retention of data will conflict with data protection principles that " personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes." To require this information to be stored will violate data protection principles and does in effect mean that millions of innocent users of communications systems, including email and the Internet, will have their private communications information stored on the off chance that it might be of use in the future. Depending on the data stored in relation to individual network users, node- holders/sys- ads may wish to warn users that they network isn't private and that they reserve the right to monitor and intercept communications; this is, of course, particularly pertinent to the Insatiably Curious Sys- Ad,

RIP Summary

42. RIP provides a mechanism by which the State can intercept citizens communications. The Act applies to both public and private networks. If a node- holder is required to disclose data to the security forces, it will be an offence to refuse to do so or to tip- off the individual involved.

43. Currently, there is a voluntary Code of Practice requiring Communication Providers to retain data on individuals' communications, this appears to conflict with the Data Protection Act 1998. It is arguable that open network holders could be communication providers, therefore it is suggested that the community become involved in lobbying to get such organisations excluded. In the authors' view, it was not the intention of the legislation to make tiny networks retain such data, but in the absence of further guidance, we highlight this as a potential future issue.

Indecent Photographs of Children and Pseudo Photographs, Obscenity

44. Node- holders and sys- ads have raised concerns as to their criminal liability if one of the network users is involved with criminal activities relating to the above, namely downloading of pornography involving children and pseudo photos of child pornography or obscenity.

45. As first enacted, the Protection of Children Act 1978 (UK) defined 4 offences:

Section 1.–

(1) It is an offence for a person–

(a) to take, or permit to be taken, any indecent photograph of a child

The Protection of Children Act 1978 introduced the concept of indecent photographs of children into UK legislation.

According to section 7 of the Act:

(2) References to an indecent photograph include an indecent film, a copy of an indecent photograph or film, and an indecent photograph comprised in a film.

(3) Photographs (including those comprised in a film) shall, if they show children and are indecent, be treated for all purposes of this Act as indecent photographs of children.

(meaning in this Act a person under the age of 16) ; or

(b) to distribute or show such indecent photographs; or

(c) to have in his possession such indecent photographs, with a view to their being distributed or shown by himself or others ; or

(d) to publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs or intends to do so.

The Criminal Justice and Public Order Act 1994 amended this to deal with the concept of pseudo- photographs. A pseudo-photograph is an image produced manually which is indistinguishable from a real photograph produced using a camera. In the UK, the Criminal Justice and Public Order Act 1994

amended the Protection of children Act 1978 so as to define the concept of an indecent pseudo- photograph of a child.

46. The Case of *Atkins & Goodland v Director of Public Prosecutions* (QBD)Wednesday 8 March 2000 Case No: CO/3417/99 relates to whether an individual was guilty of criminal offences relating to child pornography where pornographic images were stored in his browser's cache. Apparently the Defendant didn't know that the images were stored in the cache, as it was not clear whether he knew of the existence of one, therefore the criminal act was not committed unless the defendant knew that he had, or had once had, the photographs in his possession. Since it could not be shown that the defendant had been aware of the existence of the cache in the first place, he could not be guilty of being in possession of the photographs stored in the cache. So it is a requirement that the node- holder/sys- ad is aware of the photographs, i.e. they knew they had or once had the photographs in their possession. This will of course be utterly dependent on the amount of data the node- holder/sys- ad collects from the network users. Clearly the insatiably curious sys- ad may, if they see or are aware of the photographs be committing an offence, however if such data is not automatically collected by the system and is therefore not transferred to the node or cached there, the node- holder/sys- ad will not be committing any offences.

47. To like effect is the case of *R v Smith (Graham Westgarth) R v Jayson (Mike)*
[2002] EWCA Crim 683 the court held that the act of opening an attachment to an email which was known to contain pho - tographs of a naked girl amounted to the act of "making" an indecent photograph contrary to S1 (1) Protection of Children

Act 1978 notwithstanding that the image was not saved to disk or actually created by the recipient. The act of down-loading the images from the Internet to the screen of the ap-pellant's computer was an act of making an indecent photo-graph provided that the individual concerned knew about the image and intended to view it, the offence does not require an intention on the part of the maker to store the images with a view to future retrieval. However, if an image was sent as an e-mail attachment and unbeknown to the recipient, and the recipient opened it, that would not provide the requisite in-tention to complete the offence and the recipient would not be guilty.

48. Further, the case of *R v Graham Waddon* (CA) Thursday 6th April 2000 provided the authority for the principle that computers involved in the "transmission" of illegal photographs were not, or their operators, involved in the offence as those computers transmitted images but did not "produce" them, which was a required element of the offence i.e. the many computers which played a part in the transmission of material from this country to, say a website abroad and from the website abroad back to this country, were not involved in the "production" of material: they were involved in its transmission.

Obscenity Summary

49. A node-holder/sys-ad who is unaware of illegal photographs passing across the network will not be guilty of an offence. This will be particularly so if the data available to the node-holder/sys-ad is severely circumscribed. Such node-holders will be unaware of such data and it will be inaccessible to them. The node will merely be transmitting the images, not producing them.

50. However, if such data are downloaded onto the node itself, and the node- holder/sys- ad is aware of these photographs, the situation may be very different, subject to their intention and their further actions. For example, deleting the photographs/pseudo- photographs and informing the police would strongly indicate they did not have the requisite intention to commit the offence, as compared to viewing them and deleting them and then taking no further action, which may indicate they have possessed or made such images.

Defamation

51. This section is included merely for completeness ; the majority of open public networks will simply transfer data, as compared to publishing or displaying it. However, if the network incorporates some form of open web publishing facility, such as a forum or Wiki, then defamation may be an issue. In *Godfrey v Demon Internet Limited* [2001] QB 201 the respondent brought an action in defamation against the appellants, who were ISPs. They had received and stored on their news server an article, defamatory of the respondent, which had been posted by an unknown person using another service provider. The issue was whether the appellants had a defence under s1(1) of the Defamation Act 1996. The Judge held that they did not. He observed at p.208:

"In my judgement the defendants, whenever they transmit and whenever there is transmitted from the storage of their news server a defamatory posting, publish that posting to any subscriber to their ISP who accesses the newsgroup containing that posting. Thus every time one of the defendants' customers accesses soc.culture.thai and sees that posting defamatory of the plaintiff there is a publication to that customer."

52. The case of *Totalise PLC v Motley Fool LTD*, decided in February 2001, represents a further step in the law following the *Godfrey v Demon* case. This case also concerns the anonymous posting of defamatory statements on a web-based discussion board. The author of the comments used a nickname. The plaintiffs sought an order from the court requiring the defendant ISP to release information it held that could lead to the identification of "Z Dust"; the anonymous author. The defendant ISP took no responsibility for what was posted on their boards and acting quickly to remove it and ban the user. The court ordered the defendants to disclose the required information. This case demonstrates that if ISPs act expeditiously once they are notified of the presence of offensive content on their servers and remove it, they will effectively avoid liability.

Defamation Summary

53. Defamation is unlikely to be relevant to open public networks. This is simply because the network merely transmits data, and does not publish it on external websites.

Disclaimers

54. This section refers to the node-holder's duties to their network users. It is clear that network users **must** be informed in some way that the network is not private and that their data transfer is not protected. This is for two reasons: firstly, to comply with RIP, and secondly, to comply with the Data Protection Act.

55. If you are at any time are going to intercept data which, you may do for network maintenance purposes, your users must be informed that their privacy might be infringed. You may

find that a deeming provision on log-in, if you have such a page may help; for example: “On using this network you and any receiver are aware that your communications may not be private and you accept this risk on using the network.”

We would suggest that the node-holder makes clear in which way and how often their privacy could be infringed.

56. Alternatively, such information could be put somewhere visible on the premises where the node is physically located.

57. Secondly, depending on the type of open public network being operated, node-holders may find further types of disclaimers useful, such as limitation of liabilities or requiring lawful use of the Internet etc. The nature of the disclaimers will depend very much from node to node. In our view, currently, disclaimers, save for privacy, will not avert much liability. Again, if any individuals have any experience of falling foul of users due to lack of disclaimers, we would be grateful to hear from you.

58. There are numerous examples of disclaimers relating to Internet usage or virus protection or security all over the net. We recommend cutting and pasting them onto a page if you feel that you require disclaimers at all.

Disclaimer Summary

59. The network users must be informed of the node-holders' privacy policy and the likelihood of privacy intrusion.

60. General disclaimers, e.g. for limitation of liability etc., are not normally necessary, but will depend on the nature of the node and its usage.

Software Recommendations for Upholding User Privacy

61. In the course of reviewing the legislation as it applies to node-holders/sys-ads, it becomes apparent that there are certain things which must be borne in mind when deploying open public network gateways in order to respect your users' right to privacy. This is by no means a best practice document; it only specifies recommendations, which the sys-ad is free to follow or ignore.

62. From time to time it may be necessary to use a packet sniffer to diagnose problems and ensure the good functioning of the network.

    Legal provision is made for this for **businesses**, in The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, so it is clear that this was envisaged when the RIP Act was signed into law. **You should make every possible effort to let your users know that this kind of monitoring, for these reasons, may take place.** At these times the sys-ad should bear in mind the implications of intercepting anything more than packet headers; both the sender and receiver of communication must consent to such monitoring. Packet sniffers are able to capture IP addresses and also application layer data such as images or e-mail content. Running the sniffer on the gateway may also be considered part of the telecommunications system. Consider running the sniffer using a wireless interface on a laptop *instead*, as this helps to avoid the temptation of running it continuously. Remove any logs when diagnostics are complete.

63. Generally MAC addresses are insufficient information to identify individuals, as they only identify a particular wireless device, and may often easily be changed through software configuration. Private IP addresses, as specified per RFC1918,

are usually insufficient to identify individual systems as they are not globally registered. Avoid assigning private addresses to individual systems. Logging any more information than a MAC address or RFC1918 IP address in terms of network use further reduces the privacy your users have. Be aware of this if you decide to employ any method of authentication such as EAP, PPPoE or NoCat.

64. Avoid the temptation to monitor your users' use of the Internet on anything more than an aggregate basis. The default behaviour of most operating systems is to only compute aggregate input/output statistics for network interfaces. Whilst it is possible to use tools such as BPFT and Etherape to maintain per-host statistics using packet sniffing, this is more invasive than maintaining aggregate statistics, as you are readily able to see which Internet hosts your users are accessing.

65. If you wish to run a web cache such as Squid to improve overall network performance by caching frequently-used web content, be aware of the implications of doing this; please refer to the section on Obscenity for more information about this. Avoid the temptation to examine the content which is being cached directly, as this is also an invasive practice in terms of your users' right to privacy; except where such examination is essential for ensuring the continued operation of the cache as a service, for example, when setting it up for the first time.

Set-up Summary

66. Node-holders/sys-ads should ideally ensure that their users' rights to privacy are enshrined in how they choose to administer and deploy the node.

67. They should be aware of the legal responsibilities they potentially face in enlarging the scope of monitoring and logging of network activity.

68. We urge node-holders/sys-ads to exercise their responsibility with due care and diligence given the legal background explained in the rest of this document.