# Preemtory to Guardian Attacks

# Preemptory to Guardian Attacks

1<sup>st</sup> of all we are dealing with 2 things, All <u>Freedom of speech</u> 1<sup>st</sup> amendment Issues take precedence as in "in my opinion", but we are also dealing with ownership of any posted material, Copyright Law. Our case has been documented well. Please be advised that any advice that may be contained in this webpage is a simple suggestion, we take no responsibility legally nor financially should you be involved in a dispute we encourage you to seek the advice of a qualified attorney immediately.

We have thought about these things well and hard for a great while and have come to the consensus of these inherent truths.

- 1. As members of the fellowship of Narcotics Anonymous, we own the intellectual property as stipulated in the court case of (Moorehead vs. WSO) in the judges statement it expresses we hold the ownership still, (the fellowship). As it also expresses this in the FIPT documents.
- 2. that as active groups of Narcotics Anonymous we are entitled the rights afforded to us by our FIPT documentation.

Many of us have formed groups (some have registered) some not, and have decided to utilize our rights granted via the FIPT documents. Following the rules made up in our FIPT and the associated bulletins we have obtained permission to use said articles contained in this statement.

http://www.na.org/ipbul 1 rv.htm

- An NA Group shall only reproduce NA Fellowship-approved recovery literature when it has a clear need to do so. 4. The copyright for the item being reproduced should be shown prominently as follows "Copyright (c) [year of first publication by the WSO]. World Service Office, Inc. Reprinted by permission. All rights reserved."
- **5.** As long as the conditions of this IPB#1 and this IPB#4 are met, **no advance permission is required.** Groups need not, but are encouraged to, register themselves with the World Service Office. <u>also see FIPT Bulletin#4 (Revised).</u>

Many people have tried to keep the message of recovery Free, and have been directly intimidated, threatened and slandered into conforming to the will of a few select "powerful members in the service structure of our NA fellowship". The same "powerful members" have now manipulated and changed their own rules in a blatant attempt to censor the first amendment rights granted us all, they have began an terrorism attack utilizing threats of legal action, smear campaigns of character assassination amongst the fellowship, I.E. "this faction only wants to destroy what we have", or "these members are rebels and are threatening us financially".

We have dedicated this section to the ongoing saga of our battle to keep the message of recovery free.

1<sup>st</sup> Contact.... From respective complainant

## What to do if your group receives a letter

notification or cease and desist letter

First remember, the only way they can win with this tactic is;

They are required to prove that your group is not a group (in court), how can they do this? The definitions of what constitutes a group are clear and written in the Basic Text of Narcotics Anonymous. The way we respond to them can help them establish if we are a group or not. In as much it bolsters our case if we respond properly.

The NAW\$ has long stood on the premise that online groups are not legitimate, they believe that a separate standard be applied and they continue to espouse that online groups are not, they have even gone as far as refusing to register any group that has disclosed that they are an online group, thereby practicing

a unique discrimination, against the members it was designed to serve. The only reason this continues is that we (the online groups) have not formed a representative and appropriate service structure as of yet. Yet we do have in fact a strong class-action discrimination case of prejudicial treatment if we so choose to file a suit at this time. But at this time that is an option that would not be in the best interest of the NA fellowship and therefore we attempt to do everything short of such an action.

#### **WARNING**

Do not get trapped into the reverse method of being told that you have to provide NAWS with proof that you are in fact a legitimate group. The burden of proof is on them and there is NO standard method of doing this at this time. Nor are we required to disclose our business meeting minutes to the NAWS without a court order.

Suggested response; this will work well and establish unequivocally that they are in fact dealing with a group of Narcotics Anonymous. The reason for the cc to the Attorney General's office is to point out that the actions being taken are in fact in violation of the filed FIPT documents that are on file with the Attorney General's office of California.

Dear Sirs.

We received your \*request-demand-cease (whatever)\* As a representative of the \*\* group I will bring this matter before the group for review and discussion. We will address this \*\* at our next regular scheduled business meeting, as your \*\* does not justify an emergency business meeting at this time. At that time we will respond to you via Email to: <a href="world\_board@na.org">world\_board@na.org</a> & PO BOX 9999 Van Nuys, California 91409 USA as to the results of our group's conscience meeting.

Please be aware that as this is a group issue I cannot modify nor change the policy or remove content of group materials without their consent and group conscience.

Thank you,

(whoever) (GSR), (web-servant)

cc; California Attorney General, \*\* Group archives, ISP Admin.

.....

The issue at hand is one of copyright protection, and certain groups have insured that the copyright is still protected and owned by NA. The groups that have placed literature on line to my knowledge have followed the proper course of copyright law and the guidelines of the FIPT that gives them the (permission) right to do what they are doing. Should the matter get drawn out into a legal battle NAW\$ will only loose the entire issue in a prima fascia case. Any entity that gives permission in such a matter as the FIPT does, cannot possibly win a case of (copyright infringement) against a group. But they can attack the validity of the group and if they win that attack, the FIPT does not apply, that's where the attacks come from time and time again. But each time the above response is registered they cease their activities as they now realize they are in a can't win situation.

If your group does not prove to be a (non-group) then the only recourse left for them at that time is as described by the FIPT Bulletin No. 5 (revised) follows; the final line #6 is where we suggest you go. If the member, group, service board, or committee is not satisfied by the decision made by NA World Services, it can request that the conflict be resolved at the next annual meeting of the World Service Conference.

#### FIPT Bulletin No. 5 (revised)

CONFLICT RESOLUTION WITHIN THE NA FELLOWSHIP

OK What if NAWS sends out letters – Email to my ISP and threatens them?

This has been an ongoing standard procedure for the WSO officers as they actually state that there is a protected copyright being violated and they are the owners and request that the ISP 'take it down' or face charges, this is in fact a bluff but the ISP doesn't know that.

Respond immediately to the ISP when you are advised of the claim made by the NAW\$, ask for an exact copy of the complaint and whom made it. Then cite the FIPT include the facts and remind them that you are in fact the owners of the property listed on the website. Include the permission statement, and the specific addresses of the documents on the na.org website. This fast response has proven to satisfy some of the ISP's and they have left the sites alone. Some ISP's will 'cave' at the slightest threat of involvement of a suit. But some have and will continue to defend the rights your group has.

We have found that it is a good idea to advise – consult with your ISP prior to placing your Groups site on their servers, to ask the questions and pose the possible situations that may occur, for those of us who keep their ISP informed, problems like this one are easier to solve (when and if they do occur)

### What is my ISP going to do if they get served???

That's a hard one to know but if your ISP is a member of the ISP/C they have these documents to follow:

As you requested, I have prepared this memorandum to give ISP/C members general advice on when they can or cannot release information about communications and subscribers on their systems. While I have endeavored to address the most likely issues, there will certainly be details in any particular case that cannot be covered in a general memo; as a result, it is important that ISP/C members consult competent counsel if they have questions on a particular fact pattern.

#### What an ISP can and cannot do under Federal law,

The primary Federal statute in this area is the Electronic Communications Privacy Act (ECPA), which is part of the Federal criminal statutes dealing with wiretaps. ECPA generally prohibits the interception (which means any sort of acquisition of the contents of a communication by use of an electronic or other device), use, and disclosure of the contents of electronic communications. "Electronic communications" is defined in the ECPA as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce.... 18 USC 2510(12).

It is not unlawful for an officer, employee, or agent of a provider of an electronic communication service (defined in the ECPA as "any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of electronic communication, and any computer facilities or related electronic equipment for the electronic storage of such communications, whose facilities are used in the transmission of a wire communication") to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of the service or to the protection of the rights or property of the provider of the service. 18 USC 2511(2)(a)(1)

Taken together, these provisions of the ECPA permit an ISP to acquire the contents of an electronic communication on the ISP's system when that acquisition is needed to provide the underlying service (such as would be the case in tracking down mis-routed e-mail or retrieving a lost file) or to protect the ISP's system (as would be the case in examining spam or other harmful materials or pursuing unauthorized users of the system.)

In addition, providers of electronic communication services (including their officers, employees, and agents) are authorized by the ECPA to provide information, facilities, or technical assistance to persons authorized by law to intercept electronic communications if the provider is provided with either a court order directing that assistance signed by the authorizing judge, or a certification in writing by the Attorney General of the United States or the chief prosecuting attorney of a state or local unit of

government that no warrant or court order is required. An ISP who provides this sort of information and assistance under a court order or certification cannot be sued for those actions. 18 USC 2511 (2)(a)(ii) Separate from interception, the ECPA generally prohibits a provider of an electronic communication service from intentionally divulging the contents Of an electronic communication that is in transit on that service, except to the addressee or intended recipient (or that person's agent.) 18 USC 2511 (3)(a). The contents of such a communication can be divulged to a person over whose facilities the communication is forwarded, to a third party with the consent of the originator or recipient, or under a proper court order. In addition, an ISP can disclose the contents of such an in-transit communication to a law enforcement agency if the contents were obtained inadvertently and appear to pertain to the commission of a crime. 18 USC 2511 (3)(b)

The other piece of Federal law that is directly applicable is the Stored Wire and Electronic Communications and Transactional Records Access portion of the wiretap law. That statute generally prohibits a provider of an electronic communication service from knowingly divulging the contents of a communication while in electronic storage by that service, and from knowingly divulging the contents of any communication which is carried or maintained on that service. 18 USC 2702 (a)(1) and (a)(2). An ISP can divulge the contents of a communication if the ISP obtains the lawful consent of the originator, of an addressee or intended recipient, or the subscriber. An ISP can also disclose the contents of a communication without specific consent to the addressee or intended recipient of a communication (or that person's agent), to a person whose facilities are used to forward that communication to its destination, or as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service An ISP may also divulge the content when presented with a court order or certification (as discussed above), or can on its own divulge contents to a law enforcement agency if those contents were inadvertently obtained by the ISP and appear to pertain to the commission of a crime. 18 USC 2702 (b).

An ISP can disclose information about its subscribers (but not the contents of communications) to third persons other than government entities. 18 USC 2703 (c)(1)(A). (Note that this is quite different than the limitations placed on telecommunications carriers under the 1996 Telecommunications Act. Carriers have a duty to protect the confidentiality of proprietary information of customers - such as the quantity, type, destination, and amount of use of telecommunications services and information on customer bills other than customer names and addresses which are published in a directory - which Information service providers do not have unless they become telecommunications carriers.)

As with the ECPA, an ISP who provides information or assistance under the terms of a court order, warrant, subpoena, or certification is protected from civil suit. 18 USC 2703(f).

#### What an ISP may be barred from doing under state laws.

Virtually all states have adopted intrastate wiretap statutes which parallel the Federal wiretap statute. While these may be of limited value in the instance of an ISP handling inherently interstate Internet traffic, they often provide an additional basis for law enforcement to seek information and access. Some states have also adopted a version of the Stored Electronic Communications and Transactional Records Access statute (such as Minn. Stat. 626A.)

### What an ISP may be barred from doing under agreements with customers.

An ISP can agree to provide its customers with a greater degree of privacy protection than that required by Federal or state law. For example, an ISP can agree through its contracts with subscribers that the ISP will not give out subscriber information to third parties. To the extent an ISP has made

these commitments - in service contracts, in an AUP, or through postings on the ISP's system - the ISP will be expected to live up to them.

This suggests that each ISP should very carefully review the representations it has made to subscribers and/or the public about what it will and will not do with system, user, and subscriber information. If a representation has been made and a third party has relied upon that statement, the ISP will likely be liable if the representation is not followed.

### Why you don't want to intercept or divulge improperly.

A violation of the ECPA can subject the guilty party to fines and imprisonment up to five years. 18 USC 2511 (4).

A violation of the Stored Wire and Electronic Communications and Transactional Records Access statute can result in injunctive relief, damages (including potentially punitive damages), and the award of attorneys fees and court costs. 18 US 2707.

Failure to abide by promised privacy terms can subject an ISP to private suit for damages, defamation, and consumer fraud.

## What is the government required to do to get information from an ISP?

The criminal division of the Department of Justice can apply for a court order authorizing interception of communications for a wide variety of suspected crimes. 18 USC 2516. As part of the process of asking the judge to issue an interception order, the DOJ may seek the assistance of third parties, and the order can direct a provider of electronic communications to furnish "information, facilities, and technical assistance necessary to accomplish the interception..." 18 USC 2518 (4). The government is responsible for explaining to the judge the nature of the offense at issue, the sort of communications sought to be intercepted, and where and by whom the communication is being made (and thus intercepted.) No notice to anyone else is required as part of the process for securing a court interception order. 18 USC 2518 (1)

The contents of stored electronic records can be sought by the government either through a traditional warrant or through a court order. 18 USC 2703.

#### What do non-government parties need to do to get information from an ISP?

The parties to a civil lawsuit can request the judge in that case to issue a subpoena to a non-party to produce information relevant to that case or to provide testimony related to that case. In either instance, the party would fill out a fairly simple form which would be routinely issued by the judge. It is also possible for third parties to just request information from an ISP.

## Responding to subpoenas and court orders.

In almost all instances, governmental demands for interception of communications, access to communications, and access to subscriber information should be accompanied by a written court order or subpoena. The "self-certification" exception in the ECPA to the need for a court order is supposed to be for emergency situations only, and is to be accompanied by a request for a court order within 24 hours. USC 2518 (7).

In either instance, the ISP is likely to be presented with a document commanding the ISP to take specific actions or produce specific records and information, under penalty of law. There will be a date by which the action is supposed to be taken or the material produced.

## **Some practical considerations:**

Don't permit low-level employees to accept service of legal documents - only an owner or trusted manager should have the authority to accept service on behalf of the business. Letting other persons accept service may mean that deadlines begin to run while the responsible party is unaware of the

receipt of the subpoena or order. If you are presented with a subpoena or order, immediately inform legal counsel. Fax a copy of the materials to him or her, and plan to meet as quickly as possible. Do not provide information or access until you have been able to speak with counsel. While the Federal statutes provide a "safe harbor" defense for an ISP which relies on a subpoena or order, that reliance must have been in "good faith", which requires a consideration of all the facts and circumstances.

It is usually possible to ask the court to modify or withdraw ("quash" is the legal term) the subpoena or order if it is overreaching or unduly burdensome, or was for some other reason improperly issued. Any such request must be made promptly or it can be lost, so carefully review the subpoena or order and determine what would be involved in complying (if you can), how long it would take, what staff would be needed, and what it would cost. That information will be needed by counsel in assessing the best response.

It may be more productive to negotiate directly with the government office that sought the subpoena or order to frame it in a way that makes it easier to respond, and thereby avoid going to the issuing judge. Do not contact the subscriber or other persons who would be affected by the subpoena or order until you have carefully reviewed the demand with counsel; you may be forbidden to provide any notice to them. The ECPA bars an ISP from disclosing the existence of any interception, and any such improper disclosure renders the ISP liable for civil damages. 18 USC 2511 (2)(a)(ii). Under the Stored Wire and Electronic Communications and Transactional Records Access statute, you may or may not be able to inform subscribers, depending upon the information sought. 18 USC 2703 (b).

If you are asked to prepare a backup copy of the communications sought to be disclosed under the Stored Wire and Electronic Communications and Transactional Records Access statue, you must make that backup within two days of receipt of the subpoena or court order. You may not notify subscribers at the time; the government agency will provide that notice and permit the subscriber(s) to challenge the use of the materials.

Keep track of all the time you spend responding to the subpoena or court order, and any expenses you incur. An ISP that assists in an interception under the ECPA is entitled to be compensated for its reasonable expenses. 18 USC 2518 (4). An ISP that assembles information under the Stored Wire and Electronic Communications and Transactional Records Access statute is entitled to reimbursement of reasonable costs, including costs due to disruption of normal operations 18 USC 2706.

#### **Reacting to search warrants**

If a law enforcement agency decides to proceed by a search warrant, the process will be much less pleasant. It is not uncommon for law enforcement agents to appear, armed, at a business' door with a warrant to search for and seize business records, computers, and electronic records. In those circumstances, you may have little time to react, but the following suggestions may help to mitigate the damage

Alert counsel at once. While it is unlikely that he or she can prevent the search from taking place, he or she may be able to prevent it from being needlessly disruptive. You are entitled to a copy of the warrant and a receipt for any property taken. You (or your counsel) can ask for a copy of the materials (usually an affidavit) supporting the warrant, but that may have been sealed by the court and not be available to you.

Make a record of how the agents executed the warrant. If they go beyond the scope of the warrant (and it depends how precisely framed the warrant is), there may be a basis for claims against the agents. Try to record the areas searched, items seized, and any statements the agents make. Do not obstruct the search, but alert the agents if you believe they are going beyond the scope of the warrant.

If you can (and this may provoke the agents, so be careful), photograph or videotape the search and the items seized. Ask for the opportunity to copy seized materials before they are removed from your offices.

Do not engage in discussions with the agents, or make employees available to be interviewed. The agents have no right to compel employees to answer questions. It is often recommended that companies being searched send all non-essential personnel home and make all communications with the agents through one designated person.

### Responding to private requests.

Civil litigants will generally use subpoenas, and the issues discussed above should be applicable. Any direct request by a private party for access to communications or subscriber information must be carefully considered before an ISP responds. The same statutory restrictions about interception of communications and divulging of the content of communications passing through or stored on an ISP's system apply in the case of private parties. The Stored Wire and Electronic Communications and Transactional Records Access statute does permit an ISP to give non-content subscriber information to private parties, but the ISP must be sure not to violate state statutes or contractual provisions against such disclosure.

"Sweet Surrender"