

THE SPECULATIVE INVOICING HANDBOOK

First Edition

© Copyright 2009

Some rights reserved.

This work is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 Unported License.

To view a copy of this license, visit:

<http://creativecommons.org/licenses/by-nc-sa/3.0/>

or send a letter to:

Creative Commons,
171 Second Street, Suite 300,
San Francisco, California,
94105, USA.

Obtain permission before redistributing. In all cases this notice must remain intact.

Disclaimer

This document is for informational purposes only and does not provide any legal advice; it should not be interpreted as doing so. Neither the contributors, authors, publishers or distributors accept any responsibility or legal liability resulting from the use or misuse of the information presented in this document or any of the resources referred to within it.

You accept in reading this document that you do so at your own risk.

Any views and opinions expressed in this document do not necessarily represent those of the author.

Stage One: Put The Kettle On

So you've received a letter, you feel intruded upon and threatened. You're wondering if you even did what you've been accused of – well, at least, what your *connection*, has been accused of...

You're not the first and you're *unlikely* to be the last to get one of these 'nastygrams'.



The first step to managing the situation you've been put in is to tackle it calmly. You have been invited to play a game. This particular game requires careful thought and rational, planned actions. It is not best played while emotions are running high; never do anything in haste.

You're reading this handbook so you've clearly used your head so far and are on the right track.

If you've not already done so, make yourself a cuppa and sit down to read the rest of this. Relax... you're among friends now. Welcome to the team.

Photo credit: Mark Thurman
(<http://www.flickr.com/people/mthurman>)

Stage Two: Don't Make a Bad Situation Worse or Quick Advice to Get You Started

- Don't write *anything* about this for at least 48 hours... blog posts, letters, emails, forums... *nothing*. You'll figure out why later.
- Don't get drunk (yet).
- Wise man say: be selective where you go for information. In other words – there's a lot of bad advice out there. Think carefully before acting on any of it.
- Understand the ins and outs of your own situation. Only you know your own particular circumstances. No one can tell you exactly what to do. You need to review the information and make your *own* decisions.
- Play as part of a team. It's the only way you'll win this.

The Dummies Guide to Peer-To-Peer File Sharing

Peer-to-peer (sometimes referred to as P2P) file sharing is a means by which data can be shared between computers. Traditionally on the internet a home computer would have connected to a web server (typically a much more powerful computer, owned by a company or an organisation rather than an individual) to download large files that users wanted to access. These files might have been software, music or other entertainment media, documentation or any other type of file.

This model for the distribution of files evolved over time. Running servers is costly, and ensuring that the files required are available on servers depends on someone with a server making them available – something that might not be possible, for instance, for an independent musician or a lone software developer.

Peer-to-peer technology developed. When files are shared peer-to-peer there is no 'major' server. Instead, a number of the home computers connect to each other. Generally a number of these computers will hold a copy of the file desired by another user. Each of them will share a portion of the file with the person wanting it. The process is automated and the technology pretty much looks after itself as far as a download is concerned.

It may take some time to download a file. At the same time as the computer is downloading one section of the file it is quite capable of *uploading* a part it has already received to someone else who also wants it. Indeed this is the fundamental principal of file sharing. If no one uploaded no one would be able to download.

Peer-to-peer is most often publicised in a negative context – that of illegal file sharing – infringing the copyright of others. It is worth noting however that file sharing itself is not illegal, and there are many legitimate uses of the technology.

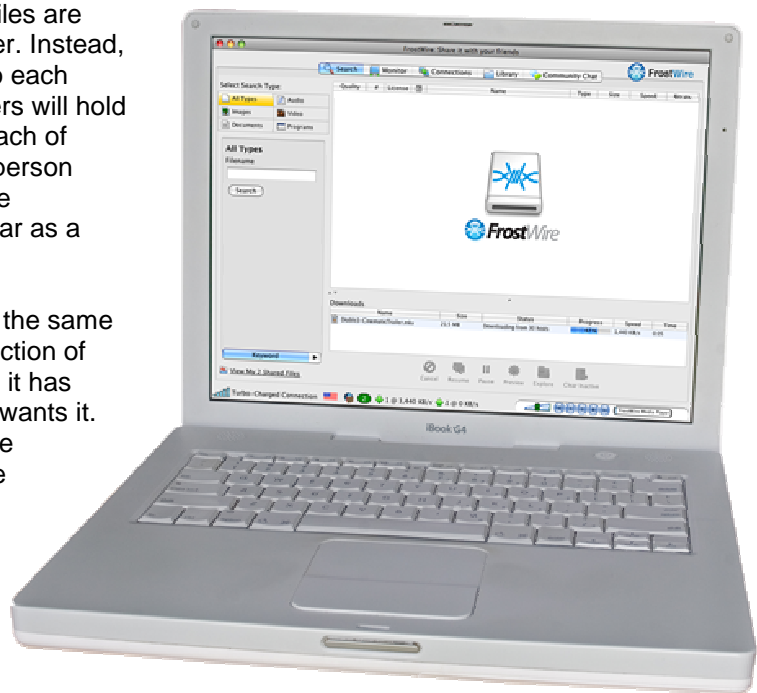


Photo credit: Nic McPhee (<http://www.flickr.com/people/nicmcphee>) and Angel Leon (<http://www.flickr.com/people/gubatron>)

The Five-Point Plan to Stop Speculative Invoicing

Take Away the Money

The letter you have received is part of a scheme designed to extract as much money as possible, from as many people as possible, as easily as possible. Do not be under the illusion that the primary intention of the scheme is to deter internet piracy. In fact, a presentation by one of the companies behind the scheme makes clear that piracy is very profitable. Claims of the type you have received can bring in 150 times the money that would have been made had a legitimately purchased copy of the work been sold.



The only reason this scheme continues to operate is that it remains profitable. Where does this profit come from? People like you – scared into paying up *by a letter designed to do just that*.

At the moment, it is claimed by one of the companies carrying out this work that 15-40% of people pay up (depending on the title in question) – no questions asked.

Without an income how much longer would the scheme last? Perhaps until they'd run out of stamps. Not much longer. People like you are their *only* source of money. It is important that you part with as little money as you possibly can. I can tell you now the exact percentage of the 60-85% of people that didn't pay that ended up in court. ZERO. The scheme relies on easy payers.

If you send them £500 consider how that will support their business. How many more letters can they afford to send with *your money*? One of them might be another letter to you...

The very fastest way we can stop this is to cut off their money. Not only is this quick and easy, it also means you save £500.

What you do: Not pay.

Hurt Their Business

The people running this scheme don't write music, they don't create games, they don't even produce pornography. They go out and they talk to people that do – the 'original rights holders'. They encourage them to sign over the distribution rights to their products.

It is with these 'distribution rights', along with some harvested IP address data that the companies running the scheme apply for their court order to get your name and address.

Some of these rights holders, in the early stages of the scheme, may not have known what they were getting involved with. The scheme has now been operating for several years. A very quick search on the law firms involved makes very clear that this is a nasty business. Any rights holder in on the scheme now can safely be considered as a willing participant in the operation.

The nature of the scheme is such that it attracts unsavoury businesses. It now focuses almost exclusively on hardcore pornography. It is important that people do all they can to make sure everyone understands what a shoddy scheme this is, and that while right owners may be tempted to sign up for a 'quick buck' in a challenging market the net result may well be a seriously (and rightly) damaged reputation and an association with some unsavoury organisations.

No-one selling rights = Nothing to pursue = No business

What you do: Do everything you legally can to take away the business of those involved. Make sure *everyone* knows how shoddy this scheme is and which 'rights holders' are in on it.

Destroy the Business Model

Further on in this handbook you will find a section that diagrammatically sets out how exactly the speculative invoicing scheme works. There are clear weaknesses in the plan; it is these that have to be exploited to stop these businesses in their tracks.

The successful operation of the scheme involves several crucial 'weak links' – without which everything falls apart. Let's look at those:

The 'pre-compliance' of your ISP

At present the majority of ISPs confer with the lawyers in advance of the application for the Norwich Pharmacal Order. They make it clear that they will not contest the application (ie. they will not question the validity of the information supplied as evidence against you). Unless they have changed their minds since the order releasing your details was signed, your ISP was one of them. Your ISP did not consider that it was worth their time or effort to protect you from the threats that they knew would follow, despite being fully aware of weaknesses of the information cited as evidence. The ISPA – the ISPs' own trade association has stated that they are "*not confident*" in the abilities of the data collectors to correctly identify copyright infringing users.

Three facts:

- An ISP is a business.
- They won't protect you because they don't think it's worth it.
- As their customer you have the perfect chance to show them they're wrong. Cost them money – ditch them – and tell them why.

In November 2009, ISP BT allowed an order to be made against them, uncontested. It related to 25,000 IP addresses. It is estimated that this will translate to approximately 15,000 BT broadband subscribers.

If 15,000 subscribers leave BT *they can't afford to ignore it*. Do it. Leave your ISP and tell them exactly why - you can't trust them to act responsibly.

It doesn't make a real difference who you choose as your new ISP so long as you make it very clear to the ISP that stitched you up why they lost you.

What you do: Ditch your untrustworthy ISP. Start your notice period NOW. And tell them why.

Income

People like you are the only people funding this unpleasant scheme. Their dependence on your money is their biggest weak point. Exploit it.

What you do: Not pay (did we say that already?)

Read Their Rules and Refuse to Play by Them

In November 2009 documents used by the companies involved in the speculative invoicing scheme were leaked onto the internet.

These documents show that the companies assign a 'litigation rating' to their victims. Essentially it highlights for them how worthwhile it is likely to be to pursue that individual. It is based on a large number of factors, few of which are related to the strength of the information presented as evidence. Primarily it is based on your own technical and legal knowledge, the potential that litigation might produce poor publicity (such as when a couple of pensioners were misidentified as files sharers of pornography) and the likely state of your finances (ie. if you have money they believe they can extract from you).

Your ISP didn't tell the company how old you are. They didn't say what your income is, if you have children, how many people live at your house, how your computer is configured, the length of your password, if you have a lawyer. Anything they know about you is either something they've found on the internet, or something you tell them.

In simple terms: *their system works because you tell them stuff.*

If you are innocent and stick to a straight denial you will be one of tens of thousands of faceless unworkable claims. The minute you tell them about you they start ticking boxes, using the information to potentially find out more about you and most importantly – you become a real person to target – something beyond the IP address they started with.

Turn out the lights. Leave them in the dark. Tell them nothing.

The only time you should provide any information is if and when they supply any evidence to support an accusation against you personally. This has never happened to date. In the event it does, see a solicitor.

An important note:

Do not rely upon knowledge of these documents to shape your reply. It is likely that if you do so it will just be obvious that you will have seen the leaked paperwork and this may not be to your advantage. However, while it is quite possible that the exact details of the paperwork will have been changed by the time this handbook is published it is clear that the companies are dependent on information from their victims to enable their scheme to operate effectively.

There are More of Us. Exploit This.

You are just one of many thousands of victims. The most effective way to have an impact is as part of a team. Keep yourself aware of developments and help the group effort where you can.

In the history of the scheme there have been many victims that have been content to sit back and let others do a lot of work on their behalf. That doesn't help. The websites you have used for information didn't happen overnight – they took work. You might have heard about the sites from a story on a news site – that'll have been the result of a press release someone wrote. All of the research, publication of leaked documents, template letters of denial, background legal information, website design and creation of resources have taken people a very considerable amount of time to produce.

Many hands make light work. While there are loads of us, please make sure you play your part. As I'm typing this handbook it's a quarter to midnight. It's work, but it's worthwhile. Do *your* bit.

Photo credit: David Jones (<http://www.flickr.com/people/dgjones>)

Top Five Frequently Asked Questions *or* Things We Ought To Make Clear

Is this a scam?

Technically this is not a scam. While the way the scheme works has much in common with a scam, the letter is genuine and is intended to be a legally valid 'Letter of Claim'. The letter you have received should not be ignored. However, this is not to say that the letter is necessarily correct, morally sound or legally indisputable.

What if I didn't do it?

There's an excellent chance that you didn't do it. The claim you have received is based on data concerning an IP address. This is connected to a piece of hardware, not an individual human being. As such it is impossible for anyone outside of a household (and possibly even those within the household) to know who committed the infringement - assuming such an infringement even occurred. Remember it has not even been possible for the ISPs to link all of the IP addresses collected by these companies to valid accounts.

Their letter of claim relies for its legal basis on the Copyright, Designs and Patents Act 1988. There are a number of factors within this act unaddressed by the letter you will have received.

Section 16(2) of the act requires a person to either directly infringe copyright, or authorise someone else to do so. They will be utterly unable to state who carried out or authorised the infringement.

It is also vital for a valid claim for it to be demonstrated that the sharing was of a whole or any substantial part of it (Part 16(3)(a) of the CDPA 1988). You will note that no evidence of this is presented. It is wholly unlikely in the case of large files, that even in the event of a work being shared a substantial part of it would have been made available from one peer, the idea behind bittorrent filesharing being that usually a number of peers will each share a small portion of the file. It would seem unlikely, given the tens of thousands of instances of infringement allegedly recorded that a full instance of the file would be downloaded and recorded as evidence to

support each claim. Their own 'Notes on Evidence' states that "As a conclusion to the monitoring process, a 'test download' was then made of the Work." This would seem to suggest that only a single copy of the work is actually downloaded to support many such claims. This would not support an assertion that a 'whole or substantial part' of it was shared from your connection.

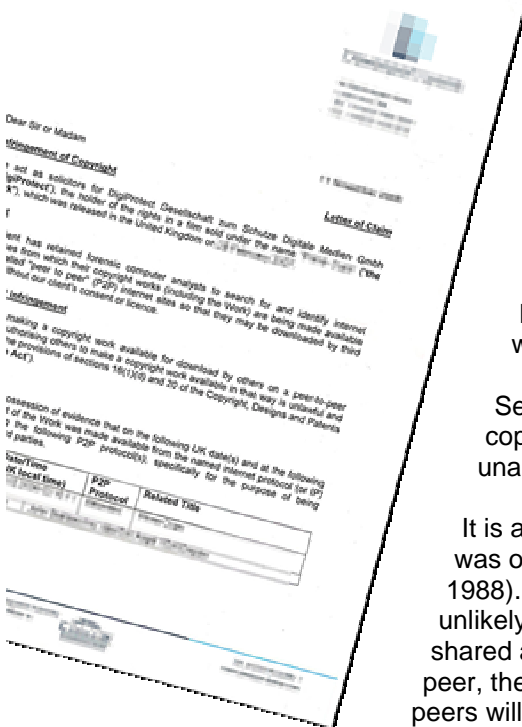
The letter of claim depends heavily upon doubletalk, missing information and the intention to provoke fear. A large part of it is hokum – particularly where claims are made that a court case is likely if you do not settle. This is demonstrably untrue.

Should I reply to the letter?

The decision is entirely yours, however, generally the advice is to at least provide a short reply.

There is a procedure in legal undertakings called 'Pre Action Protocol'. This sets out a series of very specific guidelines which should be followed in this sort of situation. The intention is that, as often as possible, cases will resolve themselves before any court action might become necessary.

The relevant document is called the 'Code Of Practice For Pre-Action Conduct In Intellectual Property Disputes' and can be found online for download.



This code states that: "The defendant should provide a full written response to the letter of claim as soon as reasonably possible. If the defendant is unable to respond within 14 days or, if the letter of claim specifies a shorter period of time, within that time period, the defendant should contact the claimant, explaining why and giving a date by which the defendant will be in a position to respond. In almost all cases a defendant will be expected to have provided a substantive response within 28 days of receipt of the letter of claim."

The code is a set of guidelines and as such you are not legally obliged to follow them, indeed, it is likely, based on past experiences, that the letter you will have received will not be wholly compliant with the code. It is a good idea to comply with the code as far as possible. In the extraordinarily unlikely event that a case ever went to court a judge would be expected to look favourably upon efforts to engage correctly in pre-action (and inversely it might be frowned upon if letters had simply been ignored).

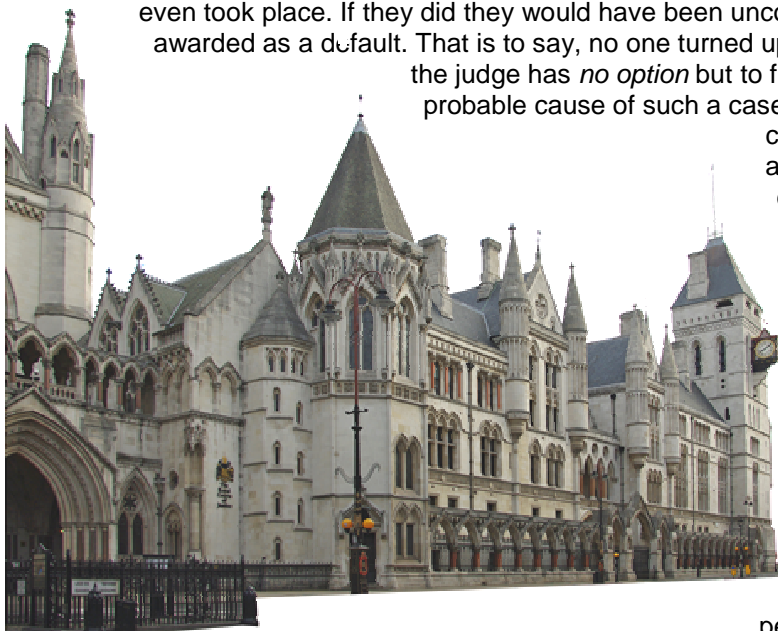
Do I need a solicitor?

Making use of a solicitor, or paying a visit to your local Citizens' Advice Bureau, is very unlikely to damage your case, however unless they are specialists in IP law, or have experience in dealing with these cases they may be of little value. The retention of a solicitor is an expense that will need to be considered in light of your own circumstances. A lazy solicitor may be inclined to simply tell you to settle, even if innocent. This would seem rather absurd.

A very considerable proportion of letter recipients (the vast majority in fact) deal with the correspondence themselves and there is no indication to date that they have been unwillingly separated from any money or suffered anything worse than those that have appointed lawyers. Generally you can just expect to receive a handful of poorly written, threatening letters.

Has anyone been taken to court? / Will I be taken to court?

Schemes of this type have been operating in the UK since 2007. In that time scores of thousands of letters have been sent. None of the letter recipients has ever seen the inside of court room in relation to one of these claims. While rumours circulate that about five cases were taken to court by a *previous* company operating the scheme in its early days, very little evidence exists to support the case that these even took place. If they did they would have been uncontested cases in which the case was awarded as a default. That is to say, no one turned up to put forward a defence, in which case the judge has *no option* but to find in favour of the claimant. The most probable cause of such a case would be letters that were ignored or not correctly delivered. A non-responder offers a good chance to the company that they can achieve a default victory. Such a case, when appropriately 'spun' offers useful publicity.



No company *currently* operating the scheme has ever taken one of these cases to court.

For more background on this topic search the internet for 'Barwinska'. Many people question if the *only person ever named* in relation to a 'court victory' (again, uncontested) of this type ever even existed. This

person was originally named only in a press release from the company operating the scheme at the time and has *never been seen* despite attempts by the press to locate her.

Will you be taken to court? You may draw your own conclusions, but it may be helpful to consider the facts of your own position (some of which you may not be aware). Within this handbook you will find information which will help you evaluate your own case.

Picture credit: Steve Thoroughgood (<http://www.flickr.com/people/andytakersdad>)

Five Big Misconceptions

This is a scam / This firm in some way aren't right

There are a whole heap of reasons why you might be inclined to reach this conclusion. The operations are certainly far from what many might consider to be professional.

You might have found other 'information' which supports the idea that one of the companies is not quite what it seems. Stuff like:

- "Their address comes up as another company!"
- "Companies House says they're dissolved!"
- "Their website isn't owned by a proper company."
- "This firm isn't registered with the Solicitors Regulation Authority."

While some of these observations may be correct, some may be partially correct - and others plain wrong, the fact remains that the letter you have received needs to be dealt with correctly. It is intended to be legally valid.

Ignoring the letter is the best way to deal with it.

In the previous chapter you'll have found a section providing an answer to the question 'Should I reply to the letter?' While the decision is entirely yours, generally advice is that a response should be provided. The letter should not be ignored.

I checked and the IP address in the letter isn't mine.

Most people do not have a 'static' (unchanging) IP address. Your router (the box with the flashing lights that connects you to the internet) will usually be given an IP address for a period of time by your ISP. This will change from time to time; this arrangement is called a 'dynamic' IP address.

You can find more information on the details of the data the companies present as evidence in a later chapter: *What You Could Fit on a Postage Stamp or Examining Their Evidence*

This is illegal!

There are some question marks concerning the legality of the process which has led to your receipt of a letter. Some of these do have a sound basis and are being investigated by the Solicitor's Regulatory Authority and other organisations. However, there have also been some ideas put forward which are incorrect.

To clarify two key points:

- A Norwich Pharmacal Order *can* be legally applied for, for use in *civil* matters. It is not necessary that a court case be started with the information ordered as a result of the NPO. In the UK it is not necessary that the application be in association with a criminal case. The assertion that the NP application process is illegal in this particular regard is incorrect.
- The rights holder may pursue their case through any legal firm and the details of your case may be passed between them. It is not illegal for action against you to have been started by one law firm and continued by another, it is the *rights holder* that is (theoretically) ordering the sending of the letters.

If I pay up they will stop bothering me.

Paying makes it clear to them that you have the financial resources to meet their demands. It also indicates that you are unwilling to fight them. It may also be interpreted as an admittance of guilt. If you sign an 'undertaking' admitting guilt, this is quite certain.

Many people have received more than one letter of claim; these may arrive at any time and may concern an entirely separate claim. They may rightly expect that if you have settled for one work you will very likely be worth pursuing in future – potentially in court.

Besides, why would you pay for something you did not do?

Innocent until proven guilty.

This is one of the most unexpected and unsettling pieces of information for newcomers to this situation who have not previously been involved in civil litigation:

'Innocent until proven guilty' is the standard of proof required in *criminal* cases (ie. brought by the state). You are being threatened with a *civil* claim. Civil cases are assessed on the 'balance of probabilities' – only a 51% likelihood of guilt is required. While (theoretically at least) this could mean that 49% of all cases assessed in this manner might be incorrectly determined that is how the system works.

Do not be unduly alarmed however. There has never been a case in the UK where someone has been found guilty of this type of infringement using solely IP address evidence. There is also no trustworthy information to suggest that the companies involved have any intention of letting a case ever see the inside of a court room.

The standard of information presented as evidence in the letter of claim you have received is really lousy.

Assess Your Position *or* Time You Knew What They (Think They) Know

If you've received a letter there are three main possibilities:

- 1) You did it
- 2) Someone else did it
- 3) No-one did it

Regardless of whether you did the deed or not, you need to know what the speculative invoicers know in order to be able to respond in a sensible manner.

They start off with extremely limited information. The first step in their process as you will know by now, is to apply to the courts to obtain your name and address (and potentially your telephone number and email address) so that they can write to you.

With any luck you'll pay up, no questions asked. If not, there's a good chance they'll invest a little time in some research. They will see if there is anything they can find to strengthen their case (because what they've got so far is next to useless).

Here's what they start with:

- An IP address
- Your name
- Your address (including postcode)
- The name of your ISP
- The name of the work shared
- The nature of the work and related works (ie. other tracks by the same artist in the case of music)

Potentially also...

- Your telephone number
- Your email address
- Knowledge of the type of router your ISP will have supplied
- A username (if the file was shared, and via eMule or eDonkey)
- A username (if you choose to post about your letter on a website using your usual username)
- Knowledge of which site made the tracker available – and the ability to collect the usernames associated with that site
- If you have participated in file sharing, knowledge of other works you may have shared or downloaded

They will use this information to scour the internet and see if they can find anything which looks incriminating. It does not matter to them whether or not anything they might potentially find is actually evidence against you or not, so long as it *looks like is*, so they can bully you with it.

You need to make sure that you are aware of what they might try to use against you. There's a reason for this. Their evidence has never yet been challenged in court, in fact the latest practitioners of the scheme have never even *tried* to take anyone to court. However, some 'court claims' have been issued. While these are simply another form of claim they do require more effort in terms of response and usually the appointment of legal representation as a defence against the claim will have to be provided. These court claims have only ever been issued against individuals against whom 'supporting evidence' could be found on the internet. In this tiny handful of cases the individuals had either admitted to file sharing openly on public internet forums or they had *appeared* to do so.

In at least one case the 'incriminating' post was actually made by another person using the same username. You do need to be aware of what information is available, even if you didn't put it there.

Assessing your position is a matter of working through a multitude of combinations and a web of interlinked information.

Consider this example:

Both of the following facts are true of our fictional character, Charlie:

- Charlie has *never* used his real name online *anywhere*
- Charlie has never admitted to file sharing the work in question online anywhere (not even under an anonymous username)

Neither of these facts stopped a case being prepared against Charlie - *a case which didn't exist until after Charlie read his letter and acted*. How strong that case might be considered is debateable.

Here is one more crucial fact concerning our fictional character:

- Charlie posted in a car-modification forum that he'd received a speculative invoicing letter

As far as this example goes that was enough to scupper Charlie. What you don't know is this:

- Unlike many of the people targeted in the speculative invoicing scheme our fictional Charlie did indeed illegally share the file in question.
- Charlie downloaded the file using eMule and left the file in his shared folder. It was therefore available for upload.
- When Charlie set up eMule (a couple of years ago) he entered a username into the software: 'sp4rky1989'
- This username was captured at the same time as his IP address was recorded as having the file available to upload.
- Charlie uses that same username on several forums on the internet – including his favourite: www.car-mods-r-us.com
- Until Charlie posted about the letter all the speculative invoicers knew was a username.
- Once Charlie had posted, all it took was a single Google search and they knew they had a match: a sp4rky1989 linked to the IP address evidence and now a sp4rky1989 that confirms he's received a letter.
- It's a hit! Let's sue!

All they had to do was search for the name of their own law firm plus a few keywords, click through a few forums and there he was. Sp4ky1989 was confirmed as *not just anyone* using the internet connection in question. It was confirmed as the account holder: Mr Charles Edward Baker, aged 21, of 36 Thorndyke Road, Thirsk, North Yorkshire.

Even if you don't consider that a confirmed username is sufficient to hold up in court; it's beyond debate that it provides a very strong incentive for a lawyer to do a lot more digging.

Charlie wouldn't necessarily have been any better off even if he didn't use eMule, or similar client. Consider another scenario (which doesn't depend upon the initial knowledge of a username):

- On an internet forum Charlie had previously posted (as sp4rky1989) about a problem he'd had obtaining an exhaust from an online supplier.
- On a completely different website (under a completely different username) Charlie had previously made posts about file sharing ("I just got a new hard drive coz this one is so chokka with warez!")
- A couple of days ago Charlie posted on a website that he'd received a speculative invoicing letter.

Your first thought might be that it would be impossible to link his post about the speculative invoicing letter to anything of use. What you don't know – and what Charlie didn't think twice about was...

Charlie's profile on the site where he discussed the exhaust included a section for interests. His included an alphabetical list of bands he liked.

This same list was reproduced by Charlie in a discussion on the file sharing site.

All the speculative invoicers had to do was note the username when Charlie made his post announcing receipt of a letter. They ran a quick search on that and found the car modification site. Looking at the profile they took a guess and ran a couple of searches; they tried the text in his signature file, the exact phrasing of his location plus a few other keywords... and they tried the text of his band list.

The band list gave them a 100% match on a file sharer. A little more digging and they would find that the locality of this file sharer (which he had discussed in the forum – though not by name) shared striking similarities with Thirsk, Charlie's town. Coincidence? Possibly, but not likely.

In this example though, it doesn't need to be two internet forums and a list of his favourite music. It could have been a part number for a headlamp and a couple of internet forums; an internet forum, a corporate website and a telephone number; a single internet post and the use of the same username; a careless registration on a website where your email address was left exposed... you get the idea.

You need to be incredibly aware of what information there is about you online, or what information appears to be about you. A postcode connects to several addresses, each with a history of residents. A telephone number is unlikely to have always been yours. Usernames are rarely unique across the internet.

Unfortunately the weak information used by the speculative invoicers to start these claims is not sufficient to use for anything other than threatening letters. The digging therefore begins... but if you happen to share 'personal' details with someone that *has* shared files then your job is that much harder.

Here are some other things that might've been true about a potential 'Charlie' that might not have occurred to you:

- His employer had posted details about Charlie on the company website, including the college he studied at, his job title, direct office telephone number, his interests and a rough outline of the work he does.
- A friend had posted Charlie's phone number on a social networking site when she was trying to arrange a meal out six months ago. She didn't realise her post could be seen, but the weak privacy settings of a friend who also posted in the thread left it wide open.
- The same page included masses of personal information about Charlie. This however, had marginally better privacy settings – only 'friends of friends'.
- Sam, a friend of Charlie, has 376 friends on the same site. Competitive friend, Ray, has 378. When a speculative invoicer, wanting more information on Charlie, using a fake profile, clicks to be added as Sam's friend – Sam accepts. Charlie is now wide open.
- Two years ago, Charlie sold a spare set of spark plugs online. The post contained his email address along with a whole host of other personal information.
- Five years ago Charlie posted a short review of an album on Amazon. The review shows both his 'verified real name' and one of his internet usernames.

The above lists represents a tiny portion of the personal information which might potentially be available online. You need to consider anything about you that makes you apparently identifiable – you've suddenly got a stalker, and an unpleasant, financially motivated one at that.

Did you yet consider?..

- Friends Reunited
- Archived news – be it on a school or company website or a local or regional media outlet
- Any social networking sites (consider if any of the following ring any bells: Facebook, MySpace, Bebo, Twitter, Friendster, Badoo, Buzznet, deviantART, Faceparty, Flixster, Geni, Habbo, Last.fm, LinkedIn, LiveJournal, MyHeritage, Netlog, Plaxo, Tagged, Tumblr, WAYN, MSN)
- Personal blogs
- Dating sites
- People search tools (such zoominfo.com and 123people.com)
- Internet forums
- Online reviews or comments
- Feedback posted to articles or blog posts
- Publicly viewable 'wish lists'

What else have you forgotten about?

That's not to say that all of these actually *will* identify you... but they could all present a problem and would need to be investigated.


If you know that you shared a file, even if it's completely unrelated, you might be tempted to delete an incriminating post...

There are at least two well-known web archives and very probably more less well-known facilities. You can't count on deleting information without trace from the internet.

You might think that on a (wholly unlikely) day in court you can deny an account on a file sharing website is yours...

...Fine...until the prosecuting barrister asks if you'd mind signing into your email account and then asks for a 'password reminder' to be sent from the incriminating account. You have one new email.

Let's put this in a nutshell:



If you shared the file, left a big trail across the internet showing you're a file sharer *and then send a letter of denial* – you're asking for trouble.

Even if you didn't share the file, know where you stand before you post anything, or reply.

How to write an LoD

Introduction

This section aims to help you write a Letter of Response (very probably a 'Letter of Denial') which will be effective. It should also guide you against some potential pitfalls and help you understand some of the content of a 'Letter of Denial' template. It goes without saying that a Letter of Denial is appropriate only if you are not responsible for (and did not authorise) the alleged copyright infringement. There is information in this document, however, which will probably be found of value even if this is not the correct response in your case.

Understand that this document is not a substitute for individual and specific legal advice, but presents a common-sense guide collated based on collective experiences and knowledge concerning the type of letter you will have received.

Before we go any further there are some important things to understand. Read each of these points carefully and take them in. *Re-read them once you've written anything you're contemplating sending as a response.* Some of them will be mentioned elsewhere in this handbook but it won't hurt to read them again.

The key points

- 1) The letter you have received is *technically legal*. It should not be ignored.
- 2) This does not mean you are obliged to pay them a penny. You are not legally obliged to pay *anything* — no court has ordered you to do so.
- 3) The type of evidence that it is stated they hold against you has never yet been tested in court. No one has ever yet appeared in court and lost against the company writing to you on the basis of this evidence.
- 4) The fact that a letter is based on a template does not stop it being legally valid.
- 5) A template letter may not fit perfectly the needs of your own case.
- 6) Give as little additional information in your response as you judge necessary to create a valid Letter of Response. Do not answer questions which have not been asked.
- 7) The company know your address and probably your name. They have been supplied with some mysterious 'evidence' which includes an IP address which your ISP has linked to your connection. Outside of that and the name of the work they allege had its copyright infringed via your connection they know almost nothing about you. Do not tell them anything you don't need to. It will not be to your benefit and may be to your disadvantage.
- 8) You should read the *Code of Practice for Pre-Action in Intellectual Property Disputes*. It's available on the internet. It's not actually that long; a lot of it is appendices that won't apply to your case.
- 9) You should read the Letter of Claim carefully. While they are largely mail-merged there have been subtle differences found between various letters. Letters regarding an infringement of copyright on a game, for example, can be slightly different to those claiming regarding pornography.
- 10) Once you've written your letter, wait for a while before you send it. Continue reading around and keeping yourself abreast of developments until a few days before your 21-day period expires. There are a couple of reasons for doing this:
 - a. You might read something around the issue you'd not heard before and you might want to go back and tweak your letter. You can't do that if it's already in the post.
 - b. The slower the process is, the greater the chance is that this 'operation' will have been shut down.
- 11) Even if the copyright of the work was infringed via your connection have they demonstrated that *you* undertook this infringement or authorised it? It is enormously unlikely that they have. At the

time of writing, no one has ever yet made known that they have received a letter where evidence has been supplied of this.

- 12) Even if the copyright of the work was infringed via your connection you are not obliged to sign the enclosed undertaking. You would be advised to seek legal advice, either through your Citizens' Advice Bureau or a recognised law firm. Negotiations with the company are not advised without fully understanding potential future implications. Bear in mind also, points (3) and (11) above.
- 13) When editing a template letter understand *why* you're changing anything you change.
- 14) Understand that a template letter is still legally valid. They may try and tell you otherwise but it's simply not the case. You are perfectly entitled to use a template letter and not change a single word if you so wish.

The Template Letter of Denial

Now let's look at a typical template letter and see what purpose the various statements serve. This example is the Letter of Denial template that most letter recipients use.

| |
|--|
| Your name <No.> Your street Your town Your county [postcode] |
| [Law Firm name] [insert mailing address here] |
| [insert date here] |
| Re: Letter of claim dated xxx concerning XXXXX ("The work") |
| Dear Sir/Madam |
| I am writing in reply to your letter of claim dated xxx stating that my connection was used in an infringement of copyright, using peer to peer networks which allegedly occurred on the date xxxx and concerns the work "XXXXX" ("the work"). |
| You assert in your letter that the infringement was apparently traced to my internet connection. I note that I am not personally being accused of the infringement, as you have no evidence to this effect. |
| Nevertheless, I categorically deny any offence under sections 16(1) (d) and 20 of |

'Letter of Claim' is the legal term for the type of letter you have been sent. Your reply will be a 'Letter of Response'.

Note that the wording of this paragraph very carefully repeats only what they have claimed. If rephrased be careful to not make mention of 'yourself' (it's all about your *connection*) and be clear that the claim is 'alleged' (with no evidence as yet supplied).

Key to note in this (and the paragraph after next) is that even if evidence were available and tested that the work was illegally shared via your connection it would be next to impossible to prove that *you* were responsible for that action. Do not, however, embellish. Any speculation about open wireless, router cloning etc is entirely irrelevant at this stage. *They* have to show that, at least in the balance of probability, *you* are legally responsible for the copyright infringement. Don't feel the need to prove their case for them, or put words into your letter that they may turn against you, or use as an excuse to write your more letters.

If you are sure that you have not illegally infringed the copyright of this work then this paragraph makes this explicit.

copy of the work in any form, nor have I distributed it, nor have I authorised anyone else to distribute it using my internet connection. I note that section 16(2) of the act requires a person to either directly infringe copyright, or authorise someone else to do so. I have done neither, and you have not provided any evidence of my doing so. As such I cannot and will not sign the undertakings as provided by you.

As you seem to be perfectly aware, it is impossible to link an IP address to a particular person or computer without further detailed analysis, which requires a level of expertise I do not possess. Furthermore the delay in your sending of a letter of claim precludes any such analysis.

You have stated that “it will be necessary for me to set out [the] reasons [for my denial]” and that “a bare denial (without further detailed explanation) will not be sufficient to change [your] view of the circumstances”. Unfortunately your failure to supply any evidence in support of a valid claim under the CDPA 1988 means that there is little to answer. Simply, you have asserted that an infringement took place which I did not carry out or authorise, and you have provided no evidence to support any assertion to the contrary. I do not have the expertise to provide a detailed explanation. As such I can only conclude that I have been a victim of foul play.

As far as I am aware, there is no law in the UK under which you could properly hold me responsible for an infringement occurring via my internet connection, without either my knowledge or permission. I would be interested to hear your legal basis for attempting to do so.

Please inform your clients that if they wish to pursue this matter, I will seek to recover all my costs to the maximum permitted by the Civil Procedure Rules.

Depending on your exact situation this section may require editing. Some people receiving letters of claim have purchased and own legitimate copies of the works about which they have received letters of claim. As such you would not claim you have never possessed a copy of the work!

Read your letter of claim carefully. You may also wish to deny, for example, sections 17 and 16(1)(a) of the CDPA 1988, depending on the content of their letter. Do be aware of what you are, and are not, denying. Check the CDPA online; it's easily Googled and actually fairly understandable for an Act of Parliament.

Do not admit anything illegal in this section. If you need to do that, seek legal advice. If parts do not apply, simply omit them.

It doesn't hurt to point out, as in the penultimate sentence, that they have provided no evidence that you have infringed their client's copyright.

The Code of Practice says that that *“if the claim is rejected, [that you] explain the reasons for that rejection, giving a sufficient indication of any facts on which [you] currently [rely on] in support of any substantive defence.”*

This paragraph in essence, points out that while you wish to deny the claim, you cannot provide substantive ‘proof of innocence’ (and indeed you should not try!). No evidence has been supplied and as such, and given your knowledge that you have not contravened the CDPA 1988, you can only state that whatever leads them to think you are responsible, is incorrect.

This points out to them that in fact they cannot hold you legally responsible for the copyright infringement and challenges their basis for doing so. When their next letter to you fails to answer this point it exposes a monumentally large weakness in their claim.

If the case were ever to go to court (a highly unlikely occurrence based on the history of this saga), this makes it clear that in the event that their claim were unsuccessful you would be seeking to recover any losses incurred during the entire process including for your time and money in responding to their letter of claim. This is limited by law, so don't bandy about random figures.

The signature of the undersigned confirms the statement provided to be accurate and legally binding under the terms required by pre-action protocol in civil law.

Yours Faithfully

[name]

This makes it apparent that your letter intends to comply with the Code of Practice – as it should.

The letter should be signed to make it legally binding.

Some further pointers:

Do not use offensive language or angry emotive language. For example you may be 'upset' or 'disturbed' by their letter, but avoid being 'outraged'.

Do not make threats (particularly 'empty' threats) or promises.

Be truthful.

Do not expose ideas to them that might form the basis of your defence if you were to go to court.

Do not libel the company. If you *must* make comment on the professionalism (for example) of the companies or people involved (which is ill-advised in any case) make explicitly clear in your wording that this is *your personal opinion*. This is particularly pertinent if your letter is to be seen by third parties, for example if you decided to send courtesy copies of your letter to a consumer or regulatory body.

Do not make any kind of 'offer' without first taking legal advice or being *exceptionally* sure what you are undertaking.

If they have made inaccurate observations in their letter it is unlikely to hurt your case to record these in your letter (for the benefit of any future court proceeding). For example, they may have made reference to an enclosure which was not supplied; point this out.

If you pay to make the letter 'go away' this may well be used as evidence against you in any potential future claims. At present the strength of their evidence has never been contested in court. It is likely that a payment received in settlement from yourself for a prior claim would be stronger evidence on a future claim than any mysterious 'evidence' which they state their client holds.

About your second (and third, and fourth?) letters...

You will, unless the operation has already been shut down, very probably receive, in due course, a second letter. The same thinking applies to writing that letter:

- Minimal content
- Straightforward repeat denial
- Note the lack of evidence; and observe that they have only reasserted their claim of the first letter
- Note that you find their letters threatening and harassing. Warn that future correspondence will be considered harassment.
- Repeat that you will seek to fully recover your costs in the event of court action
- Again note that your letter is written in accordance with pre-action protocol (the Code of Practice)

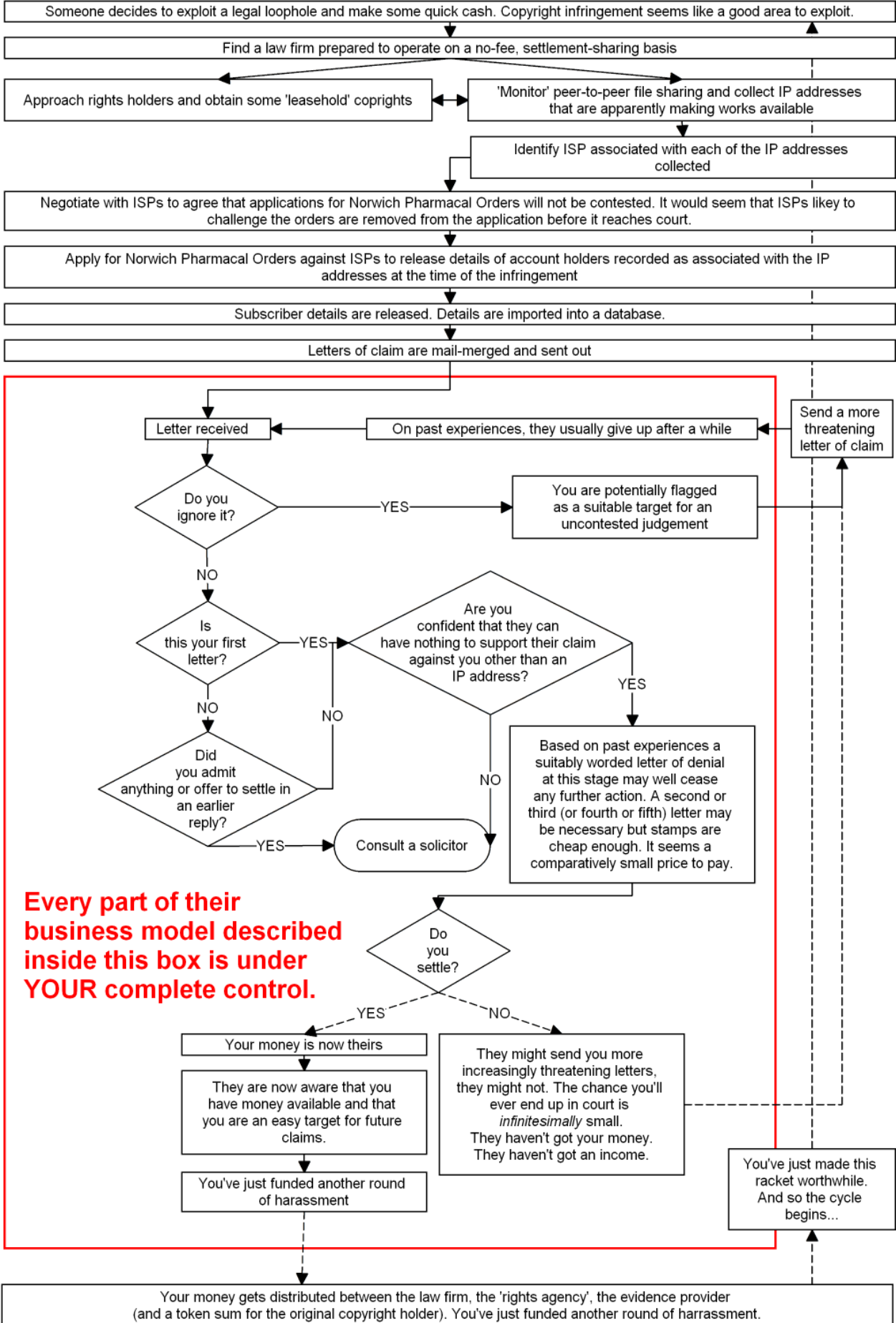
You still **do not pay**.

Understand How It Operates – The Key To Beating The Scheme

Stage 1:
Technicalities
and
Practicalities

Stage 2:
Threats

Stage 3:
Income



What You Could Fit on a Postage Stamp *or* Examining Their Evidence

All available information suggests that the 'evidence collectors' providing the type of data which have led to you receiving a letter start with some kind of (probably customised) peer-to-peer software. This connects to a collection of computers sharing a file via peer-to-peer technology (a 'swarm') and records the IP addresses of the connections which this software indicates are sharing the file.

An IP address is a bunch of numbers strung together to create a kind of temporary 'reference point' so that computers and other technological hardware can talk to each other efficiently. When you connect to the internet your hardware (the expensive stuff that you use to watch funny videos on YouTube) gets given an IP address by your Internet Service Provider (ISP).

It might look something like this:
62.252.32.12

Most people do not have a 'static' (unchanging) IP address. Your router (the box with the flashing lights that connects you to the internet) will usually be given an IP address for a period of time by your ISP. This will change from time to time; this arrangement is called a 'dynamic' IP address.

First important point: in 99.99% of cases it is *extraordinarily* likely that this is the whole of their evidence: a piece of mystery software providing a set of numbers...

The problem from them now is that having gained a record of an IP address... how should they exploit it... or rather more... *who* should they exploit with it....

The law firm correspond with your ISP (and a bunch of other ISPs – *though not all ISPs*) and tells them that they're going to apply via the courts for something called a Norwich Pharmacal Order (informally known as an 'NPO').

When the law firm apply for an NPO they present a bunch of IP addresses to the court (of which at

least one is apparently going to have been yours). They also present an 'expert witness report' kindly supplied by the 'evidence collector' (who, incidentally, are believed to get a cut of the settlements). The idea is that order, if granted, forces the ISP to release the details of the internet account holder associated with the IP address *at the time the alleged infringement was recorded by the software*.

You might think that ISPs (who fully understand the flaws in the evidence) would contest the application.

Sadly not; *most* of the ISPs roll over and play dead. Frankly they can't be bothered to object. It would appear that if there is a likelihood that an ISP would contest an application they get dropped from it before it happens. It is easier and safer for the operators of this scheme to proceed with the 'easy' ISPs than risk having their evidence challenged. Thus far this factor hasn't been enough to encourage other ISPs to do anything other than play ball with the scheming solicitors.

With no-one to contest the application (only the ISPs are entitled to do so – as the application is 'against' them) the Master (the 'judge' if you like) has little option but to grant the orders.

Somewhere up to nine months later (but usually more like 28 days) the ISPs provide all of the subscriber details requested. Well, I say 'all' – in fact only about half of the IP addresses will provide unique accounts. Some of the IP addresses will link to the same connection and some will be 'redundant' (<http://www.v3.co.uk/v3/news/2254106/bt-customers-caught-illegally>) - a handy way to say that some of the IP results are flaky enough to not even provide an attached account. ISP error? Data collection error? No one much knows. The 'reason' doesn't much matter. The fact that the evidence is demonstrably unreliable does.

