Update on enforcement actions in Europe

Armijn Hemel, MSc
armijn@tjaldur.nl

November 30, 2016

About Armijn

- using Open Source software since 1994
- MSc Computer Science from Utrecht University (The Netherlands)
- core team `gpl-violations.org` from 2005 - May 2012
- owner Tjaldur Software Governance Solutions since May 2011
- creator of the Binary Analysis Tool for compliance engineering of binary files

Today's topic: copyright trolling

Today's talk is about exploring a fairly new type of trolling: extorting money from companies disguised as GPL license enforcement, but without trying to upsell a commercial license.

Note: this is only scratching the surface and we could spend many days on it.

Talk structure

1. license enforcement background
2. reasons why license enforcement is needed
3. abuse of license enforcement
4. list solutions

Enforcement around the world

There have been open source license enforcement cases in several countries:

- France
- Germany
- Korea
- USA

Today's focus will be on enforcement of the GPL version 2 license in Germany, as that is where currently there is a lot of activity.

GPLv2 license

The GPLv2 license builds on copyright and grants many additional rights by default, unlike traditional copyright.

- made in 1991 by Free Software Foundation
- distribution license: obligations start when shipping software (either as source code, or in binary compiled form)
- license for many very popular open source packages (Linux kernel, BusyBox, Samba until 3.2.0, etc.)
- many think it is an unclear license and there is a lot of wiggling room in its interpretation (note: this is just about the *wording* of the license, not the intent)

Failure to comply with the conditions triggers an "automatic termination clause" and could lead to a copyright infringement claim.

GPLv2 enforcement cases in Germany

The automatic termination clause in GPLv2 has been used by some copyrightholders in Germany to revoke rights granted under the license and try force companies back into compliance:

- Harald Welte/gpl-violations.org (Linux kernel, iptables)
- Patrick McHardy (Linux kernel, iptables, iproute2, libnl, BusyBox)
- Christoph Hellwig (Linux kernel, this is the VMware case)

(note: this is not an exhaustive list)

Most of the cases have been about access to code and enforcing community norms.

Enforcement process in Germany

In Germany it is fairly easy to enforce the license:

- precedence (Sitecom, Fortinet, D-Link, Skype, FANTEC)
- quick and easy to get preliminary injunction
- costs (lawyer costs, engineering costs, device purchase costs) are paid by infringing party, but are generally low (or should be)

Finding evidence of infringement is often trivial (manually and/or partially automated).

Then send a cease and desist letter with a short deadline and the "legal dance" starts.

Typical problems

- no complete and corresponding source code for part or all of the software under GPLv2
- no license texts
- no valid written offer
- combinations of software released under incompatible licenses

Settlements

Most cases are settled before they go to court. The agreement for a "declaration to cease and desist" in Germany *has* to contain a clause about a contractual penalty for a future infringement: if you are caught violating again, then you have to pay the penalty. This is to encourage the defendant to take more care.

Harald Welte (gpl-violations.org) has used these penalties for donations to charities like Chaos Computer Club, Wau Holland Stiftung, Free Software Foundation Europe, etc. since his focus was on *process change*, *compliance* and *community norms*.

Aftercare

gpl-violations.org worked very closely together with Free Software Foundation Europe to get companies to talk about their problems and let them participate in the global discussion about open source compliance and other legal issues.

This worked well: gpl-violations.org (Harald, me) played “bad cop”, Free Software Foundation Europe (Shane Coughlan) played “good cop” and together we worked on process change, connecting people and actively exploring shared solutions for shared problems.

Enforcement by gpl-violations.org was always about correcting misbehaviour in the market and it worked well.

Why do we need license enforcement in the first place?

The consumer electronics industry is a mess. A few factors contributing:

- use of old and unsupported software
- sloppy supply chains
- “factory mindset”
- no understanding about open source
- cultural issues

Old software (1)

Old software (2)

The device is based on Linux 2.6.36.4:

```
Linux version 2.6.36.4brcmarm (root@asus)
  (gcc version 4.5.3 (Buildroot 2012.02) )
```

On Feb 17 2011 Greg KH said:

> *I'm announcing the release of the 2.6.36.4 kernel.*
> *All users of the 2.6.36 kernel series must upgrade.*
> *No, scratch that, you should move to the .37 kernel series as this is the last .36 kernel to be released. It's now "end of life", "dead", "buried", "pining for the fjords", or whatever term you and your company uses for things that are no more.*

This is actually one of the more reasonable ones out there. Often software that is used on consumer electronics devices released *today* is much older.

Supply chains

Multiple companies are involved in making a single product:

1. chipset manufacturer (moving higher and higher up in the software stack)
2. Original Design Manufacturer (doing increasingly less software work)
3. branding company

but there could be more parties involved:

- SDK manufacturer - commercial (example: Mentor) or open source (Yocto, buildroot, Android)
- other hardware companies (hardware drivers)

These in turn could also have sourced software from third parties.

Supply chains act as waterfalls: fixing fundamental problems downstream is very very difficult and costly (example: license enforcement).

Factory mindset

Many manufacturers operate in a "fire and forget" style: maintenance and support are minimal after release. Some companies have literally told me to "just buy the next device".

In a long supply chain this acts as a multiplier:

- chipset manufacturers stop supporting boards that their customers will actively sell for years to come.
- ODMs have standard designs that they use and adapt, but seldom update and that are used for years. Bugs discovered in one customer's product are often fixed as a "one off'.
- Bug fixes are not pro-actively pushed downstream or upstream by chipset manufacturers and ODMs.

Many devices are effectively outdated and unsupported by the time they hit the market.

No understanding about open source

Many companies in this space do not understand open source (or copyright):

- "open source" is treated as "public domain": software is renamed, or reused without even *trying* to hide the origin. After that reuse is simply *denied* despite overwhelming evidence.
- chipset manufacturers use blanket NDAs and fullfilling the license obligations for open source would breach the NDA between chipset manufacturer and ODM.
- license obligations are not met (shipping source code is actually the *exception*) and the contracts between branding company and ODM, ODM and chipset manufacturer, etc. do not take open source into account meaning there is no leverage in case of legal disputes.

Cultural issues

People do not want to take responsibility:

- branding company, ODM and chipset manufacturer all point at eachother
- process change means increased costs. Increased costs mean being unattractive to customers and margins are already quite thin. Compliance is not a feature. Security is not a feature.
- “don’t rock the boat” / “shooting the messenger”
- Avoiding face loss is a very important factor in Asia.

These factors together create a perfect breeding ground for copyright issues, but also introduce a significant security risk.

Recent enforcement cases

`gpl-violations.org` did not do any enforcement in 4 years (Harald has recently started again, but I am not involved), but since Summer 2012 Patrick McHardy has been actively enforcing his rights in Germany.

Patrick McHardy uses the same enforcement mechanisms but has a *different* motivation. He appears to be a rogue copyright troll and abuses license enforcement for personal monetary gain.

I know of dozens of companies that have been hit (some companies multiple times), although not all of them by name. He is not picky: retailers, telcos, producers, importers have all been targeted.

With his enforcement actions he has made a quite substantial income.

Patrick McHardy background

- German citizen, living on Tenerife (Spain)
- has copyrights in Linux kernel networking stack, Netfilter (firewalling in Linux kernel), iptables (user space program to interact with Netfilter), iproute2, IMQ (Intermediate Queueing Device, patch for Linux kernel), nftables, libnl and BusyBox (since 1.22.0)
- not very active in Linux kernel development for a while, but became active again in the last two years (latest commits in Linux kernel: November 2015, latest commits in nftables: late April 2016)

Differences with earlier enforcement

Enforcement done by Patrick McHardy differs from earlier cases:

- sloppy "cease and desist" letters and compliance engineering (cut/paste errors, factual errors)
- repeated enforcement in relatively short periods of time
- strange demands to put a lot of pressure on companies
- settlement talks are initiated very quickly by Patrick McHardy and his lawyer, not the defending company
- not helping companies learn more about compliance or processes, apart from a few minimal hints
- no participation in the global discussion about compliance, despite outreach by various people.

Although most cases are settled before reaching court Patrick McHardy actually has filed for preliminary injunctions.

Enforcement targets and tactics

Patrick McHardy has enforced, or addressed:

- physical products containing compiled binary code
- firmware updates from a website containing compiled binary code
- Over The Air (OTA) updates containing compiled binary code

Tactics:

1. address a (minor) violation and have a company sign a cease and desist with contractual penalty.
2. address another (minor) violation and collect the contractual penalty. Sign a new agreement with a higher penalty.
3. wait some time, then go back to 2

Devices usually have multiple issues and he only will address the "next issue" to collect the contractual penalty.

Case study: medium sized CE company (1)

In December 2013 a medium sized CE company received a letter to cease and desist from Patrick McHardy. I was hired to help them fix some things and give recommendations. The declaration to cease and desist was signed in March 2014, including contractual penalty. This was my first McHardy case.

The original claim was about 2 devices. It was a very standard cease and desist, apart from a frivolous engineering claim. I helped lower settlement costs significantly.

Case study: medium sized CE company (2)

In July 2014 a new cease and desist was sent and covered dozens of firmwares available on the support site. Some of the devices had already been off the market and firmwares were still online as a service to customers.

A per device contractual penalty of 10,000 EUR was asked, making the claim very high.

My client proposed a settlement (for far less) and McHardy didn't communicate with them for more than a year before they received another letter, with additional claims for more money.

They settled in May 2016, for a much smaller amount.

McHardy goes to court

McHardy has in the past gone to court for preliminary injunctions, hoping that some companies will be so scared by a sales ban that they will settle. This was successful at least once.

- lost at least 3 or 4 times
- won at least one time
- at least one out of court settlement

McHardy submits very large documents to court as “proof” to intimidate opponents and impress the court.

McHardy's "evidence"

McHardy's "proof" is mostly meant to scare people and waste time to make it cheaper to settle:

- source code is not annotated to separate McHardy's contributions from contributions of others
- source code is not matched with binary code and often many files from the claim letter do not even appear in the products.

Research done by various people (including myself) seems to indicate that McHardy might have written less code than he claims and might not own all the code he wrote, or claims. This is still being researched.

Copyright trolling vs patent trolling

McHardy is trolling with his copyrights, disguised as GPL enforcement.

A patent troll will sell a license for a patent and then go away. McHardy does not sell a license to his code so he can come back over and over again until you also fix all issues (real or perceived). Money will only encourage him to come back.

More trolls coming?

McHardy is the first instance of a copyright troll in open source. Rumours are floating about more copyright trolls and possible aggregation of copyrights.

Devices and solutions use code from possibly tens of thousands of copyright holders. The vast majority of these copyright holders will be friendly, but some of them could turn hostile in the future. People are starting to think about what we can do about this.

The problem of copyright trolls is currently small, but unless we fix it it will be a massive headache in the future.

Wrapping up: solutions

Solutions could include:

- technical: audits, tooling, better quality control
- legal: use better contracts
- procurement: only buy from vendors that passed an audit
- education/cultural: increase awareness about open source, create confidence, create reference materials in local languages
- community: use contributor license agreements, explore aggregation of possibly dangerous copyrights in a defensive way, identify risky individuals/companies and work around their code

Q&A