Packages - Freedom issue #1035

[your-system-sanity]: Non-Free Software From Third-party Package Managers

2016-06-19 08:03 PM - jxself

Status:	in progress	**% Done:**	0%
Priority:	feature		
Assignee:	freemor		
Category:			

Description

From a conversation on the gnu-linux-libre mailing list:

http://lists.nongnu.org/archive/html/gnu-linux-libre/2016-04/msg00070.html
http://lists.nongnu.org/archive/html/gnu-linux-libre/2016-04/msg00116.html

"A lot of programming languages have own Package Manager
Examples of those packages managers: npm (CSS/JavaScript), Bower
(Web), pip (Python), Ruby Gems (Ruby),
CPAN (Perl), Cargo (Rust), ..."

These things (like CPAN) would qualify as "repositories" under the Free System Distribution Guidelines. And they do not limit themselves to only including free software. Until/unless Stallman's ideas of either convincing them to only include free software or develop a free replacement come along I propose disabling such things in Parabola.

Related issues:

Related to Packages - Freedom issue #1413: [gnome-software][discover] offers ...	**in progress**	**2017-07-10**
Related to Packages - Freedom issue #2304: [wesnoth] Default add-ons server a...	**info needed**	
Related to Packages - Freedom issue #2260: [openttd] recommends OpenSFX, whic...	**info needed**	
Related to libretools - Feature Request #2403: [libremakepkg]: eradicate mkso...	**info needed**	

History

#1 - 2018-02-09 09:22 AM - asie

I think a better interim solution could be to patch these repository managers so that they only accept free software. However, this does not solve any privacy issues which those packages may cause, as those are not usually documented.

This shouldn't be too hard for some of them; npm for example abides by the SPDX License List standard (https://spdx.org/licenses/). Most of them seem to include licensing information in their packages, though some may not have a standardized way of denoting a specific license.

#2 - 2018-03-17 08:30 PM - bill-auger

also PECL for PHP, cabal-install for haskell, and no doubt various others

blacklisting them would be the "interim solution" - it would be a far larger set of tasks to determine how much work it would be to patch them one-by-one and then to craft and apply the patches

i will add that the FSDG actually prohibits any reference to "third-party repositories that are not committed to only including free software; even if they only have free software today" - so even filtering package according to their licenses may not be fully FSDG-compliant - and bear in mind that the license metadata in these repos is both voluntary and un-verified

as i understand, that is the main reason why parabola does not offer any tools that access the AUR repos - these language-specific repos are much of that same un-supervised, unrestrained, free-for-all sort of dumping ground for literally **whatever**

#3 - 2018-03-17 09:06 PM - bill-auger

i did a shallow survey of the guidelines for several such repos - just to determine the language they use (or neglect) to encourage proper licensing

PERL:
the PERL CPAN and repo guidelines has strong language such as "required" regarding license notices but seems to allow any license

PHP:
PHP PECL had a similarly strong requirement but with notable prescriptions regarding particular licenses; highly suggesting the 'PHP' license and even vaguely prohibiting "wrappers for GPL libraries" while allowing "Wrappers for libraries with license fees or closed sources libraries"

```
Note: wrappers for GPL (all versions) or LGPLv3 libraries will not be accepted.
Wrappers for libraries licensed under LGPLv2 are however allowed while being discouraged.
```

python and ruby:
the language of python PIP and ruby rubygems repo guidelines is significantly weaker saying only that "every package should include a license file"(PIP) and "you should specify a license"(rubygems)

rust:
although the rust cargo metadata file has a key for denoting the license; i could find no place on the web that actually recommends that anyone uses it

haskell:
the haskell cabal repo guidelines has the most libre standard of those i looked at, saying:

```
The code and other material you upload and distribute via this site
must be under an open source license
```

it then includes links to the OSI and FSF for "information about free and open source software licenses" - so perhaps 'cabal-install' is the only of this class that could be retained without conflict

#4 - 2018-04-26 12:14 AM - bill-auger

- Subject changed from Non-Free Software From Programming Language Package Managers to Non-Free Software From Third-party Package Managers

just to add - this applies not only to language-specific package managers but as well to all third-party package managers such as flatpack, appimage, docker and whatever they cook up next

#5 - 2018-04-26 12:31 AM - bill-auger

- Related to Freedom issue #1413: [gnome-software][discover] offers non-free software & shows incorrect licenses added

#6 - 2018-07-18 11:08 PM - bill-auger

let us not forget 'nuget'

#7 - 2018-11-29 10:08 PM - bill-auger

bill-auger wrote:

> let us not forget 'nuget'

i was just reminded that this "elephant in the room" applies even to guix at the intersection of "free software"/"free culture" (i.e. 'your-freedom' ^ 'your-artistic-freedom')

#8 - 2018-11-30 01:26 PM - freemor

Since we package our own pacman perhaps we could create a list of the third party package managers for it. So that if it sees a request to install those it'll throw warnings about:

```
You are installing a third party package manager!
By installing it you assume all responsibility
for system instability it may cause.
Also as doing so bypasses the Parabola blacklist.
You will have to be responsible for checking the
freedom issues of any package you choose to install
with this package manager in the future
```

or something to that effect.

#9 - 2018-11-30 01:44 PM - freemor

From where I sit using a Third party package manager is analogous to using AUR. We can't plug all these holes without creating a frustratingly restricted system. The end user needs to take some responsibility for what they install from non parabola repo places.

Yes, I do see the issue that the TPPMs (got tired of typing it out over and over) are in the Parabola repo. And could be argued as "leading people to non free...". But blacklisting the TPPMs is too restrictive and trying to patch them and then police all the packages that are improperly licensed, etc. would add a huge maintenance load.

Thus I think, Warm strongly up front about the issues possibly with a prompt requiring the user to type "Yes I understand that this may damage my systems stability and that freedom issues are my responsibility" well maybe not that long, but long enough they they have to think about what they are doing rather then just "Y <enter>" because they want to get on with what they were doing.

#10 - 2018-11-30 06:33 PM - freemor

Just a quick note:

eschwartz suggested alpm-hooks as an easy route to implement such warnings.

(mostly here so it doesn't slip from my mind if I choose to revisit this)

#11 - 2018-12-06 10:26 AM - bill-auger

freemor wrote:

> So that if it sees a request to install those it'll throw warnings about:

instead of a warning how about putting them all in a new non-default repo - with your admonishments on a new wiki page describing how to enable the repo

also, the CLI prompt is probably suppressed by pacman GUI front-ends - we could patch octopi but thats not the only one

freemor wrote:

> From where I sit using a Third party package manager is analogous to using AUR.

so should we put AUR GUIs in the new repo with the same warning? - that would seem to be one step in the opposite direction of this issue - it is surely not an omission that there are no AUR helpers in parabola - i think it is clear that AUR helpers, container fetchers, and other package managers should be treated as equivalent - (with the haskell PM being the notable exception above)

freemor wrote:

> blacklisting the TPPMs is too restrictive and trying to patch them

i think a small number of these specify license in metadata - in theory, someone could write a filter - that would be the ideal "rescue" option - still this is several such non-trivial patches against several unfamiliar projects

#12 - 2018-12-06 01:12 PM - freemor

Excellent point about GUI PMs. Living on the CLI I often forget about the GUIs

Separate Repo is an interesting idea. And yes I'd vote to fire AUR helpers in there too. One could easily argue that having a point and click AUR package manager is "helping people install non-free..."

I do understand about the metadata in some TPPMs. My worry is that not only would the be the patching/maintaining burden that you mentioned to filter, but also a whole layer of then having to police those collections for projects with improper licensing data in their metadata.

#13 - 2019-02-09 06:40 AM - bill-auger

i was just re-reading the FSDG today and it struck me as being quite clear on this issue:

```
Nor should the distribution refer to third-party repositories that are not committed to only
including free software; even if they only have free software today, that may not be true
tomorrow. Programs in the system should not suggest installing nonfree plugins, documentation,
and so on.
```

so again, from my shallow research so far, it looks that the haskell cabal is the only one that we could consider to be "committed to only including free software"

#14 - 2019-02-09 07:11 AM - bill-auger

and FWIW, i also read the original discussion on the FSDG mailing list that occurred about a month before this issue was open, in which RMS suggested that if the repositories themselves could not be convinced to distribute free software only, then the best solution would be to extract the licensing information from each of these package manager's repo indices, if possible, and import only the free packages into a new separate repo for each package manager - that, he also suggested could be hosted by the FSF, if volunteers could accomplish the work of automated filtering

https://lists.nongnu.org/archive/html/gnu-linux-libre/2016-04/msg00116.html

#15 - 2019-02-27 08:03 PM - bill-auger

- Priority changed from freedom issue to discussion

#16 - 2019-02-27 08:18 PM - bill-auger

- Priority changed from discussion to freedom issue

#17 - 2019-02-27 08:18 PM - bill-auger

- Status changed from open to confirmed

#18 - 2019-04-28 11:08 PM - bill-auger

- Related to Freedom issue #2304: [wesnoth] Default add-ons server allows non-free add-ons added

#19 - 2019-04-28 11:10 PM - bill-auger

- Related to Freedom issue #2260: [openttd] recommends OpenSFX, which is known to be under a non-FSDG license added

#20 - 2019-07-21 04:15 PM - bill-auger

- Priority changed from freedom issue to feature

- Subject changed from Non-Free Software From Third-party Package Managers to [your-system-sanity]: Non-Free Software From Third-party Package Managers

freemor has been working on an idea tentatively named 'your-system-sanity' to present a more blatant warning about the software that TPPMs index and assist downloading, and the havoc they (especially pip) can wreak on the system, and to identify and isolate them all from the main repos, possibly into new repo like: [unsupported]

though its perhaps not as ideal of a solution that curated repos shared by other distros would be; it is better than the current situation

#21 - 2019-07-21 04:15 PM - bill-auger

- Assignee set to freemor

- Status changed from confirmed to in progress

#22 - 2019-08-01 02:25 AM - bill-auger

- Related to Feature Request #2403: [libremakepkg]: eradicate mksource() from abslibre added