

Transparency in Processing of Public Information

NREGASoft, a software solution currently in use by Ministry of Rural Development, Govt of India, that intends to introduce transparency to the activities of Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS) is heavily dependent on proprietary encoding of public information by using proprietary non-free software. NREGASoft, thus, is itself in a paradoxical situation, unfaithful to the theme, while it attempts to introduce transparency in MGNREGS, of which processing of digital information itself, is considered to be a very vital component.

It is already known that there are ways of encoding public information using (open) standards which will ensure that any such information encoded using standards will always be available in future. This is because standards are published through a judicial process by a well recognised international standards body with no authors or owners for such standards, once they are released in public domain. When there are no authors or owners for standards, it is implied that ownership is public, i.e., owned by everyone.

Any other type of encoding of information which do not conform to these guiding principles, violate or dilute them, is understood to be a proprietary encoding of information resulting in a proprietary format. They are thus to be appreciated as non-standards. Terminologies like "de-facto standards", "proprietary standards", "patented standards which involve royalty", etc may qualify as oxymorons.

In a computing environment, too, there are different ways by which information can be processed, that are revealed by the license under which the software is released or distributed. It is known that software licenses are capable of restricting freedom of at four different levels. If software license restricts the user from using the software for any purpose in any number of machines, then the license is considered to violate the first level of freedom. If the license restricts the user to analyse or study the software by preventing access to the source code, it is considered to violate the second level of freedom. If the license restricts the user to make copies of software and distribute them, it is considered to violate the third level without diluting any of these four levels of freedom), it is considered to violate the fourth level of freedom. Software that respects these four levels of freedom are known as Free Software (or Free and Open Source Software - FOSS).

Therefore a truly transparent software computing environment that is involved in processing of public information, essentially needs to use (open) standards as well as process such standardised information using Free Software. A recent development on the hardware front reveals tendencies by certain hardware vendors to use proprietary firmware as part of hardware. This defeats the purpose of ensuring complete transparency. Therefore, to ensure a safe, secure and transparent environment, it goes without saying that the hardware components too need to be completely open. Only then can a user ensure that no details of its processing are hidden in a non-transparent manner.

Some of the advantages of adherence by public bodies engaged in processing public information, to such a transparent philosophy of computing are appended below. As holders of public information and as its legal guarantors, the State is expected to guarantee the citizens

- (a) permanent access to public information,
- (b) permanent availability of public information and
- (c) security of public information.

Permanent access to public information is possible only if the encoding of information or its processing is not tied to a monopoly service provider. Ensuring usage of software licenses that are compatible with Free Software will ensure permanent access to public information.

Permanent availability of public information is possible only if public information is encoded using (open) standards.

Security of public information is possible only if citizens are able to ensure that no part of the software or hardware contain hidden code (spy ware) that allows unwanted transmission of information without authorisation. Ensuring that source code is available for inspection and the freedom to compile the requisite binaries from their sources will ensure security of public information.

From the discussions above, it would be evident that NREGASoft, in its existing form cannot justify the cause of transparency which it purports to achieve, as it operates in a non-free software environment with no conclusive way of ensuring that even encoding of public information is as per established standards. It needs to be re-developed in a Free Software environment, and more so, as Microsoft Inc, whose software server components are used in the software, cannot be expected to release their software under open public licenses as Free Software.