

IS DIGITAL INCLUSION A GOOD THING? HOW CAN WE MAKE SURE IT IS?

Richard Stallman

President, Free Software Foundation

ABSTRACT

Activities directed at “including” more people in the use of digital technology are predicated on the assumption that such inclusion is invariably a good thing. It appears so, when judged solely by immediate practical convenience. However, if we also judge in terms of human rights, whether digital inclusion is good or bad depends on what kind of digital world we are to be included in. If we wish to work towards digital inclusion as a goal, it behooves us to make sure it is the good kind.

Index Terms— copyright, freedom, sharing, War on Sharing, software patents, free software, free/libre software, proprietary software, surveillance, back doors, censorship, software as a service, digital restrictions management, DRM

Copyright 2009 Richard Stallman

This paper is released under the Creative Commons Attribution Noderivs 3.0 license.

1. INTRODUCTION

Digital information and communication technology offers the possibility of a new world of freedom. It also offers possibilities of surveillance and control which dictatorships of the past could only struggle to establish. The battle to decide between these possibilities is being fought now.

Activities directed at “including” more people in the use of digital technology are predicated on the assumption that such inclusion is invariably a good thing. It appears so, when judged solely by immediate practical convenience. However, if we judge also in terms of human rights, the question of whether digital inclusion is good or bad depends on what kind of digital world we are to be included in. If we wish to work towards digital inclusion as a goal, it behooves us to make sure it is the good kind.

The digital world today faces six major threats to users’ freedom: surveillance, censorship, proprietary software, restricted formats, software as a service, and copyright enforcement. A program to promote “digital inclusion” must take account of these threats, so as to avoid exposing its intended beneficiaries to them. First we look at the nature of these threats; then we propose measures to resist them, collectively and individually.

2. SURVEILLANCE

Digital surveillance systems are spreading. The UK uses computers with cameras to track all car travel. China plans to identify and photograph everyone that uses an Internet cafe.¹ Cell phones are Big Brother’s tools. Some can be activated by remote command to listen to the user’s conversations without giving any sign of listening, by the police² and by unauthorized individuals.³ Users are unable to stop this because the software in the phone is not free/libre, thus not under the users’ control.

Cell phones also localize the user, even when set to “idle.” The phone network needs must know roughly where the phone is located in order to communicate with it, and can easily record that information permanently. However, networks are designed to locate phones far more accurately by triangulation. They can do it even better with GPS in the phone, with or without the user’s consent.

In many countries, universal digital surveillance does not record what you say, only who you talk with. But that is enough to be quite dangerous, since it allows the police to follow social networks. If a known dissident talks with you by phone or email, you are a candidate for labeling as a dissident. It is no use ceasing to communicate by phone or email with fellow dissidents when a dictator takes power, because his secret police will have access to records of your past communications.

The European Union mandates keeping records of all phone calls and email for periods up to two years. The stated purpose of this surveillance is to “prevent terrorism.” Bush’s illegal surveillance of phone calls also cited this purpose. Non-state-sponsored terrorism is a real danger in a few countries, but the magnitude is often exaggerated; more people died in the US in September 2001 from car accidents than from terrorism, but we have no Global War on Accidents. By contrast, the practice of labeling political opposition as “terrorists,” and using supposed “anti-terror” laws to infiltrate and sabotage their activities, threatens democracy everywhere. For instance, the US Joint Terrorism Task Force infiltrated a wide range of political opposition groups⁴

¹See <http://www.theaustralian.news.com.au/story/0,25197,24510571-2703,00.html>.

²See http://www.schneier.com/blog/archives/2006/12/remotely_eavesd_1.html.

³See <http://www.firstcoastnews.com/news/local/news-article.aspx?storyid=84936>.

⁴See <http://www.aclu.org/safefree/spyfiles/>

False accusations of “terrorism” are standard practice for suppressing political opposition. In the US, protesters who smashed windows at the 2008 Republican National Convention were charged with of “terrorism.”⁵ More recently, Iran described protesters demanding a new election as “terrorists.”⁶ The generals who ruled most of South America in the 1970s offered precisely that justification for their systematic murder of dissidents.⁷

A free society does not guarantee anonymity in what you do outside your home: it is always possible that someone will notice where you went on the street, or that a merchant will remember what you bought. This information is dispersed, not assembled for ready use. A detective can track down the people who noticed you and ask them for it; each person may or may not say what he knows about you. The effort required for this limits how often it is done.

By contrast, systematic digital surveillance collects all the information about everyone for convenient use for whatever purpose, whether it be marketing, infiltration, or arrest of dissidents. Because this endangers the people’s control over the state, we must fight against surveillance whether or not we oppose current government policies. Given of the surveillance and tracking cell phones do, I have concluded it is my duty to refuse to have one, despite the convenience it would offer. I have few secrets about my own travels, most of which are for publicly announced speeches, but we need to fight surveillance even if it is established while we have no particular secrets to keep.

The UK car travel surveillance system has already been used against political dissidents.⁸

3. CENSORSHIP

When the topic of Internet censorship is mentioned, people are likely to think of China, but many supposedly freedom-respecting countries have imposed censorship. Denmark’s government has blocked access to a secret list of web pages. Australia’s government wants to do likewise, but has met strong resistance, so instead it has forbidden links to a long list of URLs. Electronic Frontiers Australia was forced, under threat of fines of AUD 11,000 per day, to remove a link to an anti-abortion political web site.⁹ Denmark’s secret list of forbidden URLs was leaked and posted on Wikileaks; that page is now on Australia’s banned list.¹⁰ Germany is on the

24011res20060131.html.

⁵See http://democracynow.org/2008/9/4/eight_members_of_rnc_activist_group.

⁶See <http://abcnews.go.com/international/story?id=7891929>.

⁷See the documentary, *Condor: the First War on Terror*, by Rodrigo Vázquez (2003).

⁸See http://news.bbc.co.uk/2/hi/programmes/whos_watching_you/8064333.stm.

⁹See http://www.computerworld.com.au/article/302161/watchdog_threatens_online_rights_group_11k_fine?fp=16&fpid=1.

¹⁰See <http://www.smh.com.au/articles/2009/03/17/1237054787635.html>.

verge of launching Internet censorship.¹¹

Censorship of the contents of web sites is also a threat. India just announced a broad plan of censorship that would effectively abolish freedom of the press on the Internet.¹²

Some European countries censor particular political views on the Internet. In the United States, people have been imprisoned as “terrorists” for running a web site which discussed actions taken against experiments on animals.¹³

Another common excuse for censorship is the claim that “obscene” works are dangerous. I agree that some works are obscene; for instance, the gruesome violence in the movie *Pulp Fiction* revolted me, and I will try never to see such a thing again. But that does not justify censoring it; no matter how obscene a work may be, censorship is more so. A variant of this excuse is “protecting children,” which plays to the exaggerated and mostly misplaced fears of parents.¹⁴

Censorship is nothing new. What is new is the ease and effectiveness of censorship on electronic communication and publication (even where a few wizards have ways to bypass it). China in 1960 achieved effective censorship by cutting its population off from the world, but that held back the country’s development, which was painful for the regime as well as for the population. Today China uses digital technology to achieve effective political censorship without cutting itself off in other ways.¹⁵

4. SOFTWARE YOU CAN’T CONTROL

In order for computer users to have freedom in their own computing activities, they must have control over the software they use. This means it must be *free software*, which I here call “free/libre” so as to emphasize that this is a matter of freedom, not price.

A program is free/libre if it gives the user these four essential freedoms:¹⁶

0. Freedom to run the program as you wish.

1. Freedom to study the source code, and change it to make the program do what you wish.

2. Freedom to redistribute and/or republish exact copies. (This is the freedom to help your neighbor.)

3. Freedom to distribute and/or publish copies of your modified versions. (This is the freedom to contribute to your community.)

¹¹See <http://netzpolitik.org/2009/the-dawning-of-internet-censorship-in-germany/>.

¹²See <http://timesofindia.indiatimes.com/India/Govt-gearing-up-to-gag-news-websites/articleshow/4562292.cms>.

¹³I support medical research using animals, as well as abortion rights. Our defense of political freedom should not be limited to causes we agree with.

¹⁴See <http://www.mcclatchydc.com/homepage/story/28029.html>.

¹⁵See <http://www.networkworld.com/news/2009/052909-20-years-after-tiananmen-china.html>.

¹⁶See <http://gnu.org/philosophy/free-sw.html>.

When software is free/libre, the users control what it does. A non-free or *proprietary* program is under the control of its developer, and functions as an instrument to give the developer control over the the users. It may be convenient, or it may not, but in either case it imposes on its users a social system that keeps them divided and helpless. Avoiding this injustice and giving users control over their computing requires the four freedoms. Freedoms 0 and 1 give you control over your own computing, and freedom 3 enables users to work together to jointly control their computing, while freedom 2 means users are not kept divided.¹⁷

Many argue that free/libre software is impossible on theoretical economic grounds. Some of them misinterpret free/libre software as “gratis software”; others understand the term correctly, but either way they claim that businesses will never want to develop such software. Combining this with a theoretical premise such as “Useful software can only be developed by paying programmers,” they conclude that free software could never exist. This argument is typically presented elliptically in the form of a question such as, “How can programmers make a living if software is free?” Both premises, as well as the conclusion, contradict well-known facts; perhaps the elliptical questions are meant to obscure the premises so people will not compare them with the facts.

We know that free software can be developed because so much of it exists. There are thousands of useful free programs,¹⁸ and millions of users¹⁹ run the GNU/Linux²⁰ operating system. Thousands of programmers write useful free software as volunteers.²¹ Companies such as Red Hat, IBM, Oracle, and Google pay programmers to write free software. I do not know even approximately how many paid free software developers there are; studying the question would be useful. Alexandre Zapolsky of the free software business event Paris Capitale du Libre (<http://www.paris-libre.org>) said in 2007 that the free software companies of France had over 10,000 employees.

Most computer users use proprietary software, and are accustomed to letting a few companies control their computing. If you are one of them, you may have accepted the view that it is normal and proper for those companies, rather than you, to have control. You may also believe that “reputable” developers will not use their power to mistreat you. The fact is that they do.

Microsoft Windows has features to spy on the user,²² Digital Restrictions Management (DRM) features designed to stop the user from making full use of his own files,²³ and an all-

purpose back door with which Microsoft can forcibly change the software in any way at any time.²⁴ Microsoft can alter any software, not just its own.²⁵ Cell phones tied to particular phone networks may give the network a similar back door. MacOS also has DRM features designed to restrict the user.

The only known defense against malicious features is to insist on software that is controlled by the users: free/libre software. It is not a perfect guarantee, but the alternative is no defense at all. If code is law, those governed by it must have the power to decide what it should say.

5. RESTRICTED FORMATS

Restricted file formats impose private control over communication and publication. Those who control the formats control, in a general sense, society’s use of information, since it can’t be distributed or read/viewed without their permission.

For instance, text files are often distributed in the secret Microsoft Word format, which other developers have only imperfectly been able to decode and implement. This practice is comparable to publishing books in a secret alphabet which only officially approved scribes know how to read. Italian public television (RAI) distributes video in VC-1 format, whose specifications are available only under nondisclosure agreement from the Society of Motion Picture and Television Engineers. Ironically, the SMPTE states this in Word file, which is not suitable to cite as a reference.²⁶ This standard has been partly decoded through reverse engineering.

Most music distribution on the Internet uses the patented MP3 format, and most video uses patented MPEG-4 formats such as DIVX and H.264. VC-1 is also patented.²⁷ Any software patent directly attacks every user’s freedom to use her computer. Use of patented data formats is comparable to mandating that people use officially approved scribes rather than do their own reading and writing. Patents on MPEG formats have been used to attack and threaten developers and distributors of programs that can handle these formats, including free/libre programs. Some distributors of the GNU/Linux system, for instance Red Hat, do not dare to include support for these programs.

A restricted format is a trap; any and all use of the format has the effect of pushing computer users into the trap. Inclusion in dependence on these formats is not a step forward.

¹⁷See <http://www.gnu.org/philosophy/why-free.html> and <http://www.gnu.org/philosophy/shouldbefree.html> for other arguments.

¹⁸See <http://directory.fsf.org>.

¹⁹See http://en.wikipedia.org/wiki/Linux_adoption.

²⁰See <http://gnu.org/gnu/gnu-linux-faq.html>.

²¹See <http://www.gnu.org/philosophy/fs-motives.html> for some of their motives.

²²See http://www.theregister.co.uk/2003/02/28/windows_update_keeps_tabs/.

²³See <http://badvista.org>.

²⁴See <http://www.informationweek.com/news/showArticle.jhtml?articleID=201806263>.

²⁵See http://voices.washingtonpost.com/securityfix/2009/05/microsoft_update_quietly_insta.html.

²⁶The standard in machine-readable form is only available to be “leased”; http://www.smpete.org/standards/LicenseAgreement_CD-ROM.pdf.

²⁷See http://www.mpegla.com/news/n_06-08-17_pr.pdf.

6. SOFTWARE AS A SERVICE

Typical proprietary software gives you only a binary, whose actions are controlled by the developer, and not by you. A new practice called “software as a service,” or “SaaS,” gives you even less control. With SaaS you don’t even get a copy of the program you can run. Instead, you send your data to a server, a program runs there, and the server sends you back the result. If users have a binary, they could reverse-engineer it and patch it if they are really determined. With SaaS, they can’t even do that.

Reverse engineering being so difficult, perhaps software as a service is little worse than proprietary software. The point, however, is that it is no better. For users to have control of their computing, they must avoid SaaS just as they must avoid proprietary software.

For the preparation of this paper I was invited to use an IEEE site called `pdf-express.org` to convert my PDF file into one with the embedded fonts required for the conference proceedings. Looking at that site, I concluded that it was an instance of software as a service, and therefore I should not use it. Another strike against it is that it requires users to identify themselves, which is gratuitous surveillance.

It’s not that I’m specifically worried that this site is malicious. I cannot trust the IEEE implicitly, since I disapprove of its restrictions on redistributing the papers it publishes, but there is little scope in that particular site’s job for intentional mistreatment of its users (aside from the gratuitous surveillance). However, the point is not whether this particular site abuses its power. The point is that we should not let ourselves become accustomed to granting others that sort of power over us. The habit of handing over control of our computing to others is a dangerous one. The way to resist the practice is to refuse invitations to follow it.

The only way to maintain your control over your computing is to do it using your own copy of a free/libre program.

7. COPYRIGHT AND SHARING

The biggest conflict over freedom in the Internet is the War on Sharing: the attempt by the publishing industry to prevent Internet users from enjoying the capability to copy and share information.

Copyright was established in the age of the printing press as an industrial regulation on the business of writing and publishing. The aim was to encourage the publication of a diversity of written works. The means used was to require publishers to get the author’s permission to publish recent writings. This enabled authors to get income from publishers, which facilitated and encouraged writing. The general reading public received the benefit of this, while losing little: copyright restricted only publication, not the things an ordinary reader could do, so it was easy to enforce and met with little opposition. That made copyright arguably a beneficial system for the public, and therefore legitimate.

Well and good—back then.

7.1. The War on Sharing

Nowadays, computers and networks provide superior means for distributing and manipulating information, including published software, musical recordings, texts, images, and videos. Networks offer the possibility of unlimited access to all sorts of data—an information utopia.

The works that people use to do practical jobs, such as software, recipes, text fonts, educational works and reference works, must be free/libre so that the users can control (individually and collectively) the jobs that they do with these works. That argument does not apply to other kinds of works, such as those which state what certain people thought, and artistic works, so it is not ethically obligatory for them to be free/libre. But there is a minimum freedom that the public must have for all published works: the freedom to share exact copies noncommercially. Sharing is good; sharing creates the bonds of society. When copying and sharing a book was so difficult that one would hardly ask such a large favor, the issue of freedom to share was moot. Today, the Internet makes sharing easy, and thus makes the freedom to share essential.

One obstacle stands in the way of this utopia: copyright. Readers and listeners who make use of their new ability to copy and share published information are technically copyright infringers. The same law which formerly acted as a beneficial industrial regulation on publishers has now become a restriction on the public it was meant to benefit.

In a democracy, a law that prohibits a popular and useful activity is usually soon relaxed. Not so where corporations have more political power than the public. The entertainment companies’ lobby is determined to prevent the public from taking advantage of the power of their computers, and has found copyright a suitable tool. Under their influence, rather than relaxing copyright rules to permit productive and free use of the Internet, governments have made it stricter than ever, forbidding the act of sharing.

The publishers and their friendly governments would like to go to any length they can get away with to wage the War on Sharing. In the US, the record companies’ legal arm (the RIAA) regularly sues teenagers for hundreds of thousands of dollars, and one sharer was fined almost two million.²⁸ The French government recently passed a law (HADOPI) to abolish the principle of due process of law, by punishing Internet users with disconnection on the mere accusation of copying. Only certain selected, government-approved organizations were empowered to make such accusations; thus, this law meant to abolish *Liberté, Egalité, and Fraternité* with one blow. The law was rejected as unconstitutional by the Constitutional Council.²⁹ A similar law in New Zealand was withdrawn this year after public protests. The European Parliament recently voted against imposing similar injustice on the whole European Union, but the EU’s weak form of democ-

²⁸See <http://arstechnica.com/tech-policy/news/2009/06/jammie-thomas-retrial-verdict.ars>.

²⁹See <http://www.laquadrature.net/fr/hadopi-is-dead-three-strikes-killed-by-highest-court>.

racy does not give Parliament the final decision. Some would like to go even further: a UK member of parliament proposed ten years' imprisonment for noncommercial sharing.

The US, Canada, the European Union, and various other countries are engaged in negotiating the "Anti-Counterfeiting Trade Agreement." The negotiations are secret, but Canada reluctantly published a list of suggestions it received from private parties, and HADOPI-style punishment without trial was one of them.³⁰ The suggestion is likely to have come from the copyright lobby, which has great influence in the US government and others, so the danger is not negligible. European officials may seek to use this treaty to circumvent the European Parliament, following a practice known as "policy laundering."

The corporations that profit most from copyright legally exercise it in the name of the authors (most of whom actually gain little). They would have us believe that copyright is a natural right of authors, and that we the public must suffer it no matter how painful it is. They call sharing "piracy," equating helping your neighbor with attacking a ship.

Public anger over these measures is growing, but it is held back by propaganda. Terms such as "piracy,"³¹ "protecting authors" and "intellectual property,"³² and claims that reading, viewing or listening to anything without paying is "theft," have convinced many readers that their rights and interests do not count. This propaganda implicitly assumes that publishers deserve the special power which they exercise in the name of the authors), and that we are morally obliged to suffer whatever measures might be needed to maintain their power.

7.2. Digital restrictions management

The publishers aim to do more than punish sharing. They have realized that by publishing works in encrypted format, which can be viewed only with software designed to control the users, they could gain unprecedented power over all use of these works. They could compel people to pay, and also to identify themselves, every time they wish to read a book, listen to a song, or watch a video. They could make people's copies disappear on a planned schedule. They could even make copies unreadable at will, if they have all-purpose back-doors such as found in Windows, or special features for the purpose.³³

Designing products and media to restrict the user is called Digital Restrictions Management, or DRM.³⁴ Its purpose is an injustice: to deny computer users what would otherwise be their legal rights in using their copies of published works.

³⁰See <http://arstechnica.com/tech-policy/news/2008/11/canadian-wish-list-for-secret-acta-treaty-long-varied.ars>.

³¹See gnu.org/philosophy/words-to-avoid.html.

³²See <http://gnu.org/philosophy/not-ipr.html> for why this propaganda term is harmful.

³³See <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>.

³⁴Those publishers, in an act of doublespeak, call it "Digital Rights Management".

Its method is a second injustice, since it imposes the use of proprietary software.

The publishers gained US government support for their dream of total power with the Digital Millennium Copyright Act of 1998 (DMCA). This law gave publishers power, in effect, to write their own copyright rules, by implementing them in the code of the authorized player software. Even reading or listening is illegal when the software is designed to block it.

The DMCA has an exception: it does not forbid uses that qualify as "fair use." But it strips this exception of practical effect by censoring any software that people could use to do these things. Under the DMCA, any program that could be used to break digital handcuffs is banned unless it has other comparably important "commercially significant" uses. (The denial of validity to any other kind of significance, such as social or ethical significance, explicitly endorses business' domination of society.) Practically speaking, the limited right to disobey your software jailer is meaningless since the means to do so is not available.

Similar software censorship laws have since been adopted in the European Union, Australia, and New Zealand, and other countries. Canada has tried to do this for several years, but opposition there has blocked it. The publishers' lobbies seek to impose these restrictions on all countries; for instance, the US demands them in trade treaties. WIPO (the World "Intellectual Property" Organization) helps, by promoting two treaties whose sole point is to require laws such as these. Signing these treaties does no good for a country's citizens, and there is no good reason why any country should sign them. But when countries do sign, politicians can cite "compliance with treaty obligations" as an excuse for software censorship.

We still have the same old freedoms in using paper books and other analog media. But if e-books replace printed books, those freedoms will not transfer. Imagine: no more used book stores; no more lending a book to your friend; no more borrowing one from the public library—no more "leaks" that might give someone a chance to read without paying. No more purchasing a book anonymously with cash—you can only buy an e-book with a credit card, thus enabling computerized surveillance—and public libraries become retail outlets. That is the world the publishers want for us. If you buy the Amazon Kindle (we call it the Swindle) or the Sony Reader (we call it the Shreader for what it threatens to do to books), you pay to establish that world.

8. SUPPORTING THE ARTS

The publishers tell us that a War on Sharing is the only way to keep art alive. Supporting the arts is a desirable goal, but it could not justify these means. Fortunately, it does not require them either. Public sharing of copies tends to call attention to obscure or niche works: when Monty Python put its video files on the net for download, its sales increased by a factor

of over 200.³⁵ Meanwhile, digital technology also offers new ways to support the arts.

8.1. Donations

The singer Jane Siberry (now known as Issa) offered her music for download through her own web site, allowing people to pay whatever amount they wish. (The site, sheeba.ca, currently says it is being redesigned but suggests the general policy will continue.) The average price paid per song was more than the \$.99 that the major record companies charge.³⁶

Bestsellers also can still do well without stopping people from sharing. Stephen King got hundreds of thousands of dollars selling a serialized unencrypted e-book with no technical obstacle to sharing of copies. Radiohead made millions in 2007 by inviting fans to copy an album and pay what they wished, while it was also shared on the Internet. In 2008, Nine Inch Nails released an album with permission to share copies and made 750,000 dollars in a few days.³⁷

Even hampered by today's inconvenient methods of sending money to artists, voluntary contributions from fans can support them. Kevin Kelly, former editor of Wired Magazine, estimates the artist need only find approximately 1,000 true fans in order to earn a living from their support.³⁸

But when computer networks provide an easy anonymous method for sending someone a small amount of money, without requiring a credit card, voluntary support for artists will become far more effective. Every player could have a button you can press, "Click here to send the artists one dollar." (The optimal amount may vary between countries; in India, one rupee might be a better choice.) Wouldn't you press it, at least once a week?

Why, today, would you hesitate to send one dollar to an artist, once a week or even once a day? Not because you would miss the dollar, but because of the inconvenience of sending it. Remove the inconvenience, and voluntary support for artists will soar.

8.2. Tax-based support

Another way to support the arts is with tax funds: perhaps with a special tax on blank media or Internet connectivity, or with general revenue.³⁹ If this is to succeed in supporting artists, the state should distribute the tax money directly and entirely to them, and make sure it cannot under any pretext be taken from them by publishers such as record companies. Thus, in order to design this tax system to achieve the valid

goal of "supporting the arts," we must first reject the misguided goal of "compensating the rights-holders."

The state should not distribute this tax money in linear proportion to popularity, because that would give most of it to superstars, leaving little to support all the other artists. I therefore recommend using a function whose derivative is positive but tends towards zero, such as cube root. With cube root, if superstar A has 1000 times the popularity of successful artist B, A will get 10 times as much money as B. (A linear system would give A 1000 times as much as B.) This way, although each superstar still gets a larger share than other artists, the superstars together will get only a small fraction of the funds, so that the system can adequately support a large number of fairly popular artists. This system would use its funds efficiently for the support of art.

I propose this system for art because art is where the controversy is. There is no fundamental reason why a tax-based system should not also be used to support functional works that ought to be free/libre, such as software and encyclopedias, but there is a practical difficulty in doing so: it is common for those works to have thousands of coauthors, and figuring out the right way to divide the funds among them might be difficult even with the cooperation and generosity of everyone involved. Fortunately it appears not to be necessary to solve this problem, because people already put so much effort into developing free/libre functional works.

Francis Muguet⁴⁰ and I have developed a new proposal called the Mécénat Global (or Global Patronage) which combines the idea of tax-support and voluntary payments.⁴¹ Every Internet subscriber would pay a monthly fee to support certain arts that are shared on the Internet. Each user could optionally divide up to a certain maximum portion of her fee among her choice of works; the funds for each work would be divided among the creative contributors to the work (but not the publishers). The totals thus assigned to various artists would also provide a measure of each artist's popularity. The system would then distribute the rest of the money on the basis of that popularity, using a cube-root or similar tapering-off function.

9. MAKING DIGITAL INCLUSION GOOD

The paper so far describes the factors that can make digital inclusion good or bad. These factors are part of human society and subject to our influence. Beyond just asking whether and when digital inclusion is a good thing, we can consider how to make sure it is good.

9.1. Defending freedom legally

Full victory over the threats to digital freedom can only be achieved through changes in laws. Systematic collection or retention of information on any person using computers

³⁵See <http://www.boingboing.net/2009/01/23/monty-pythons-free-w.html>.

³⁶See <http://www.37signals.com/svn/posts/419-jane-siberrys-you-decide-what-feels-right-pricing>.

³⁷See <http://www.boingboing.net/2008/03/05/nine-inch-nails-made.html>.

³⁸See http://www.kk.org/thetechnium/archives/2008/03/1000_true_fans.php.

³⁹See <http://gnu.org/philosophy/dat.html> for my 1992 proposal.

⁴⁰Head of the Knowledge Networks and Information Society lab at the University of Geneva.

⁴¹See <http://mecenat-global.org>.

and/or networks should require a specific court order; travel and communication within any country should normally be anonymous. States should reject censorship and adopt constitutional protections against it. States should protect their computing sovereignty by using only free software, and schools should teach only free software in order to carry out their mission to educate good citizens of a strong, free and cooperating society.

To respect computer users' freedom to operate their computers, states should not allow patents to apply to software or (more generally) using computers in particular ways. States should mandate their own use of freely implementable, publicly documented formats for all communication with the public, and should lead the private sector also to use only these formats. To make copyright acceptable in the network age, noncommercial copying and sharing of published works should be legal. Commercial use of DRM should be prohibited, and independently developed free software to access DRM formats should be lawful.

To make these changes in laws happen, we need to organize. The Electronic Frontier Foundation (eff.org) campaigns against censorship and surveillance. End Software Patents (endsoftpatents.org) and the League for Programming Freedom (progfree.org) campaign against software patents. The Free Software Foundation campaigns against DRM through the site DefectiveByDesign.org.

9.2. Defending freedom personally

While we fight these legislative battles, we should also personally reject products and services designed to take away our freedom. To resist surveillance, we should avoid identifying ourselves to web sites unless it is inherently necessary, and we should buy things anonymously—with cash, not with bank cards. To maintain control of our computing, we should not use proprietary software or software as a service.

Above all, we should never buy or use products that implement DRM handcuffs unless we personally have the means to break them. Products with DRM are a trap; don't take the bait!

9.3. Defending others' freedom

We can take direct action to protect others' freedom in the digital world. For instance, we can remove the passwords from our wireless networks—it is safe, and it weakens government surveillance power. (The way to protect the privacy of our own Internet communications, to the extent that it is possible, is with end-to-end encryption.) If others use enough of the bandwidth to cause actual inconvenience, we need to protect ourselves, but we can try gentle methods first (such as talking with the neighbors, or setting a password occasionally for a day or two), and keep the option of a permanent password as a last resort.

When we publish, we should grant the users of our work the freedoms they deserve, by applying an explicit license appro-

priate to the type of work. For works that state your thoughts or observations, and artistic works, the license should permit at least noncommercial redistribution of exact copies; any Creative Commons license is suitable. (I insisted on such a license for this article.) Works that do functional jobs, such as software, reference works and educational works, should carry a free/libre license that grants users the four freedoms.

9.4. Inclusion in freedom

In our efforts to help others in practical ways, we must avoid doing them harm at a deeper level. Until freedom is generally assured in Internet use, projects for digital inclusion must take special care that the computing they promote is the freedom-respecting kind. This means using free/libre software—certainly not Windows or MacOS. This means using free, documented formats, without DRM. It also means not exposing the supposed beneficiaries to surveillance or censorship through the computing practices to which they are being introduced.