Open Hardware

Sebastian Büttrich
IT University of Copenhagen
Network Startup Resource Center

ICTP March 2017
ITU.dk
NSRC.org

Open Hardware / General Idea

To create and share

Free Hardware

Relation to Open and Free Software

The Open Hardware Movement has its background in

Open Source Software Movement.

Like in Software,
There is a debate of terms:

What is Open?
What is Free?
Is being Open enough?

The four freedoms (of software)

Simplified:

The freedom ...

1/ to run / use

2/ to study / hack

3/ to spread / distribute

4/ to change / improve

Differences to Software

In **software**, the code/the document
is the product.
In **hardware**, the code/the document
is a means to make a product.

Software tends to be about **license / intellectual property.**
Hardware tends to be about **Trademark / Certification.**
(
The line is not quite clear – today, in computing and technology,
Almost no hardware comes without a software aspect,
And vice versa.
)

What is being shared?

Hardware design in the form of
mechanical drawings,
schematics,
bills of material,
PCB layout data,
HDL source code
integrated circuit layout data,
STL,
gcode,

in addition to the software that drives the hardware, are all released under **free/libre terms**.

History

1997 Bruce Perens

Announcing: The Open Hardware Certification Program

- *To*: debian-announce@lists.debian.org
- *Subject*: Announcing: The Open Hardware Certification Program
- *From*: bruce@debian.org
- *Date*: Tue, 26 Aug 97 13:26 PDT
- *Message-id*: <m0x3SBl-00JaLkC@golem.pixar.com>
- *Reply-to*: Bruce Perens <bruce@debian.org>

```
You are getting this message because you subscribed to the debian-announce
mailing list. Unsubscription instructions are at the bottom of this message.



                Software in the Public Interest
                           announces
            THE OPEN HARDWARE CERTIFICATION PROGRAM

Supported by: Uniforum, Free Software Foundation, Linux International
and its Member Companies: Digital Equipment Corporation, Redhat
Software, Caldera, WorkGroup Solutions, Yggdrasil Computing,
Metrolink, Linux Hardware Solutions, InfoMagic, VA Research, Xi
Graphics, Tower Technology, Just Logic Technologies, Specialized
Systems Consultants H&L Software, Pacific HiTech, Quant-X Service &
Consulting Ges.m.b.H., Sebit Ltd, Tech-X Consulting, SW Technology
Enhanced Software Technologies, Prime Time Freeware

The Open Hardware Certification Program is a self-certification
program for hardware manufacturers. By certifying a hardware device as
Open, the manufacturer makes a set of promises about the availability
of documentation for programming the device-driver interface of a
specific hardware device. While the certification does not guarantee
that a device driver is available for a specific device and operating
system, it does guarantee that anyone who wants to write one can get
the information necessary to do so. There is no charge to participate
in the program. Vendors of certified equipment have the right to apply
the "Open Hardware" logo to their packaging, and to state in advertising
```

History

Perens a.o. 1997

http://openhardware.org/ (abandoned)

Background: Debian, Open Source Software

Open Hardware initially addressed primarily Computing, networking, machines ....

Cern OHL

http://ohwr.org/projects/cernohl/

HOME PROJECTS LICENSES COMPANIES

CERN OPEN HARDWARE LICENCE

http://Ohanda.org

OH&A

OHANDA.ORG

OPEN SOURCE HARDWARE AND DESIGN ALLIANCE

http://Oshwa.org

Open Source Hardware Association

https://de.wikipedia.org/wiki/Open-Source-Hardware

Respect Your Freedom

RYF/FSF

The FSF maintains a "Respects Your Freedom" (RYF) hardware certification program. To be granted certification, a product must use 100% Free Software, allow user installation of modified software, be free of back doors and conform with several other requirements. Currently, a total of eight products have been granted the certification, including three laptops, a 3D printer, a wireless router, and three USB interface wireless adapters.

The eight certified products are:

The Libreboot X200 laptop
The Libreboot X60 laptop (formerly known as the Gluglug X60)
Aleph Objects, Inc. LulzBot 3D printers
The ThinkPenguin TPE-NWIFIROUTER Wireless-N Broadband Router
The ThinkPenguin TPE-N150USB Wireless N USB
The ThinkPenguin TPE-N150USBL Wireless USB adapter
The Tehnoetic wireless USB adapter for GNU/Linux-libre (TET-N150)
The Taurinus X200 laptop by Libiquity

Licenses

“Noteworthy licenses include:

The TAPR Open Hardware License: drafted by attorney John Ackermann, reviewed by OSS community leaders Bruce Perens and Eric S. Raymond, and discussed by hundreds of volunteers in an open community discussion

Balloon Open Hardware License: used by all projects in the Balloon Project

Although originally a software license, OpenCores encourages the LGPL

Hardware Design Public License: written by Graham Seaman, admin. of Opencollector.org

In March 2011 CERN released the CERN Open Hardware License (OHL) intended for use with the Open Hardware Repository and other projects.

The Solderpad License is a version of the Apache License version 2.0, amended by lawyer Andrew Katz to render it more appropriate for hardware use.”

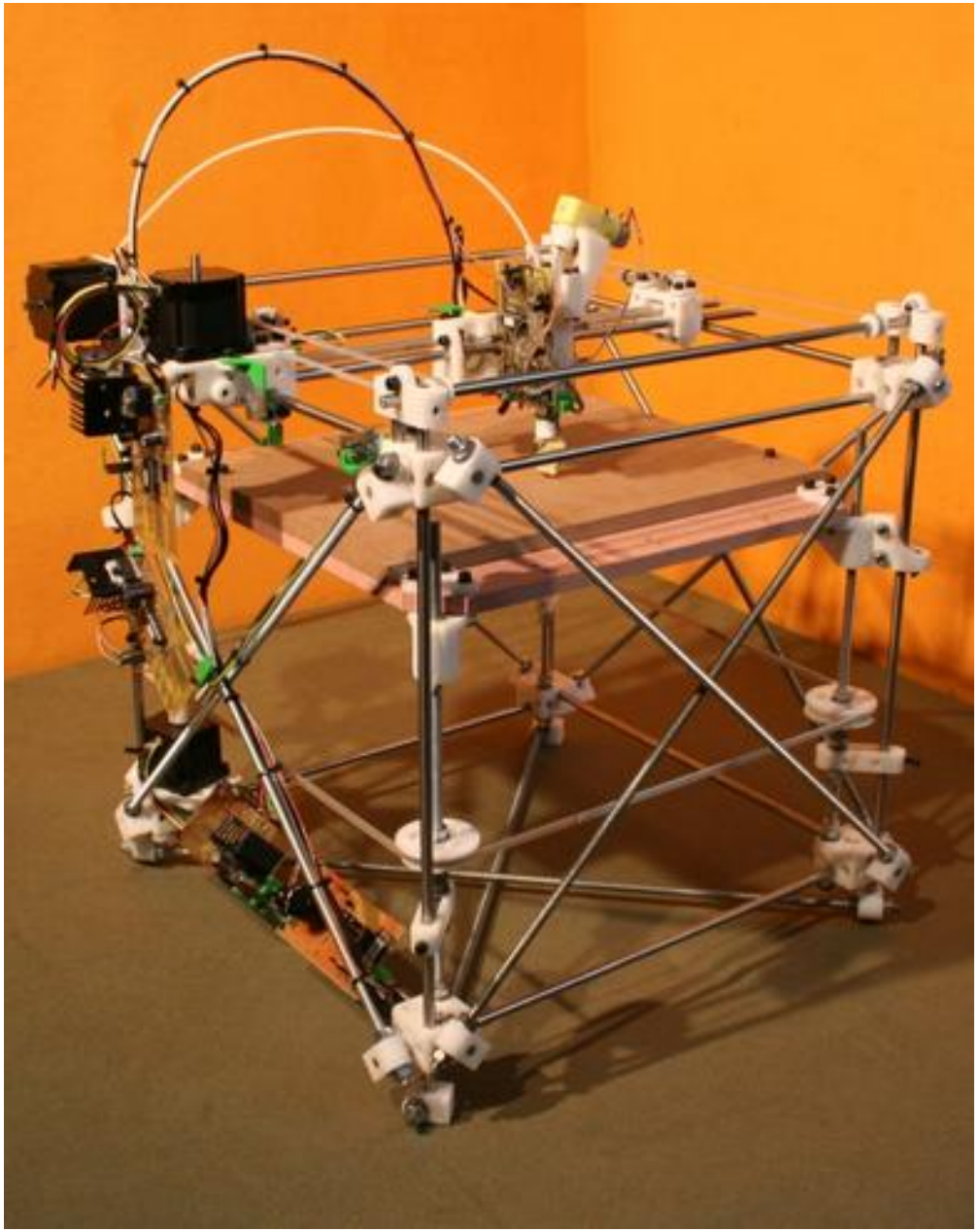
https://en.wikipedia.org/wiki/Open-source_hardware

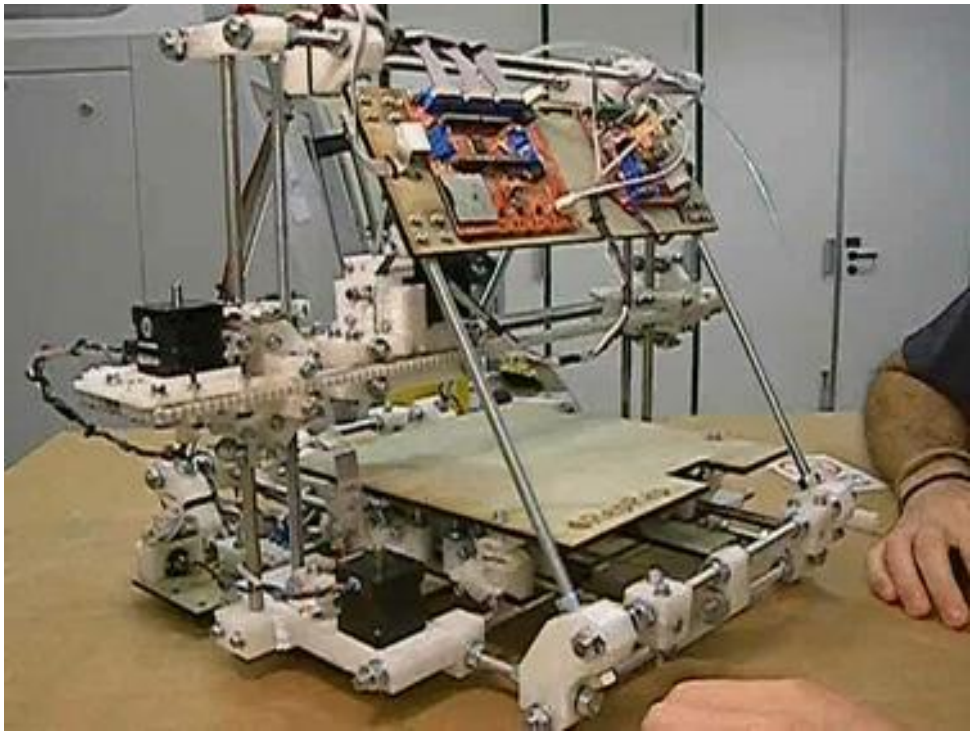
Licenses

“The Open Source Hardware Association recommends seven licenses which follow their open-source hardware definition.[34] From the general copyleft licenses the GNU General Public License (GPL) and Creative Commons Attribution-ShareAlike license, from the HW specific copyleft licenses the CERN Open Hardware License (OHL) and TAPR Open Hardware License (OHL) and from the permissive licenses the FreeBSD license, the MIT license, and the Creative Commons Attribution license. [35] Openhardware.org recommended in 2012 the TAPR Open Hardware License, Creative Commons BY-SA 3.0 and GPL 3.0 license.”

https://en.wikipedia.org/wiki/Open-source_hardware

Examples: Reprap 3D printer

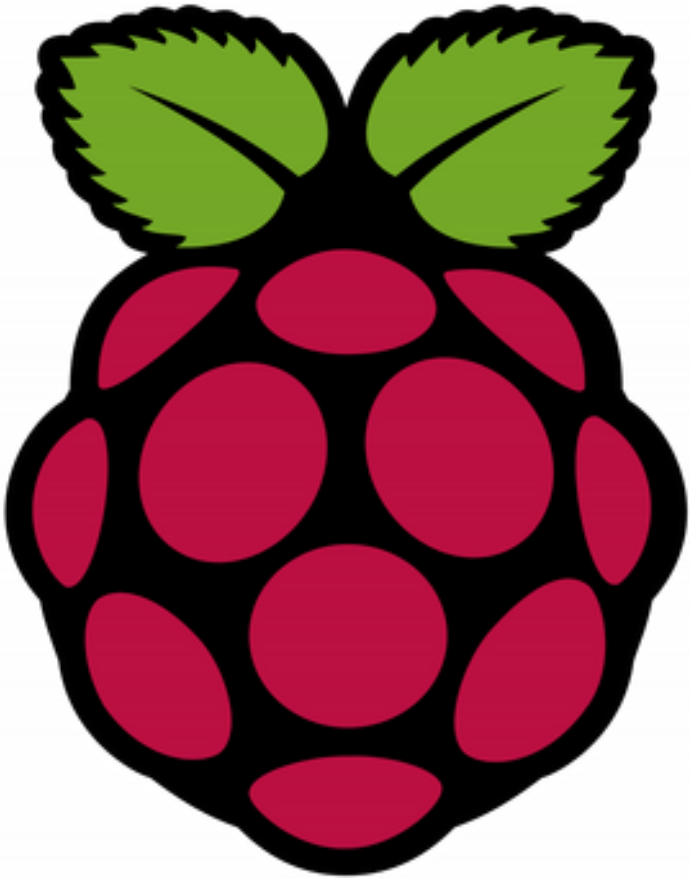




Examples: OpenCores

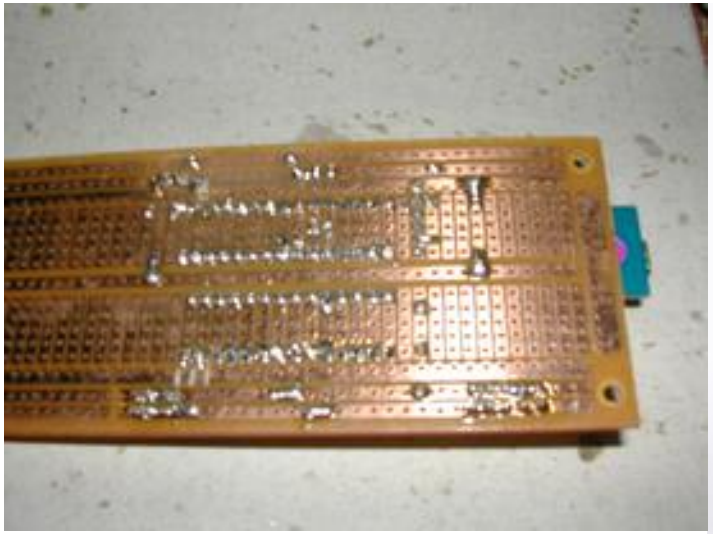
Examples: Raspberry Pi?

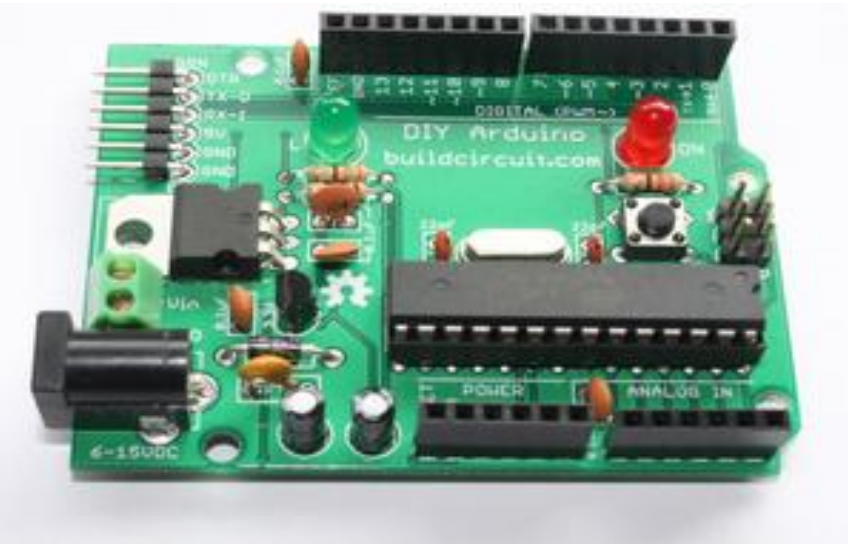
While there is a lot of open and free software within the Raspberry Pi ecosystem,
The hardware itself is not under any open hardware license.



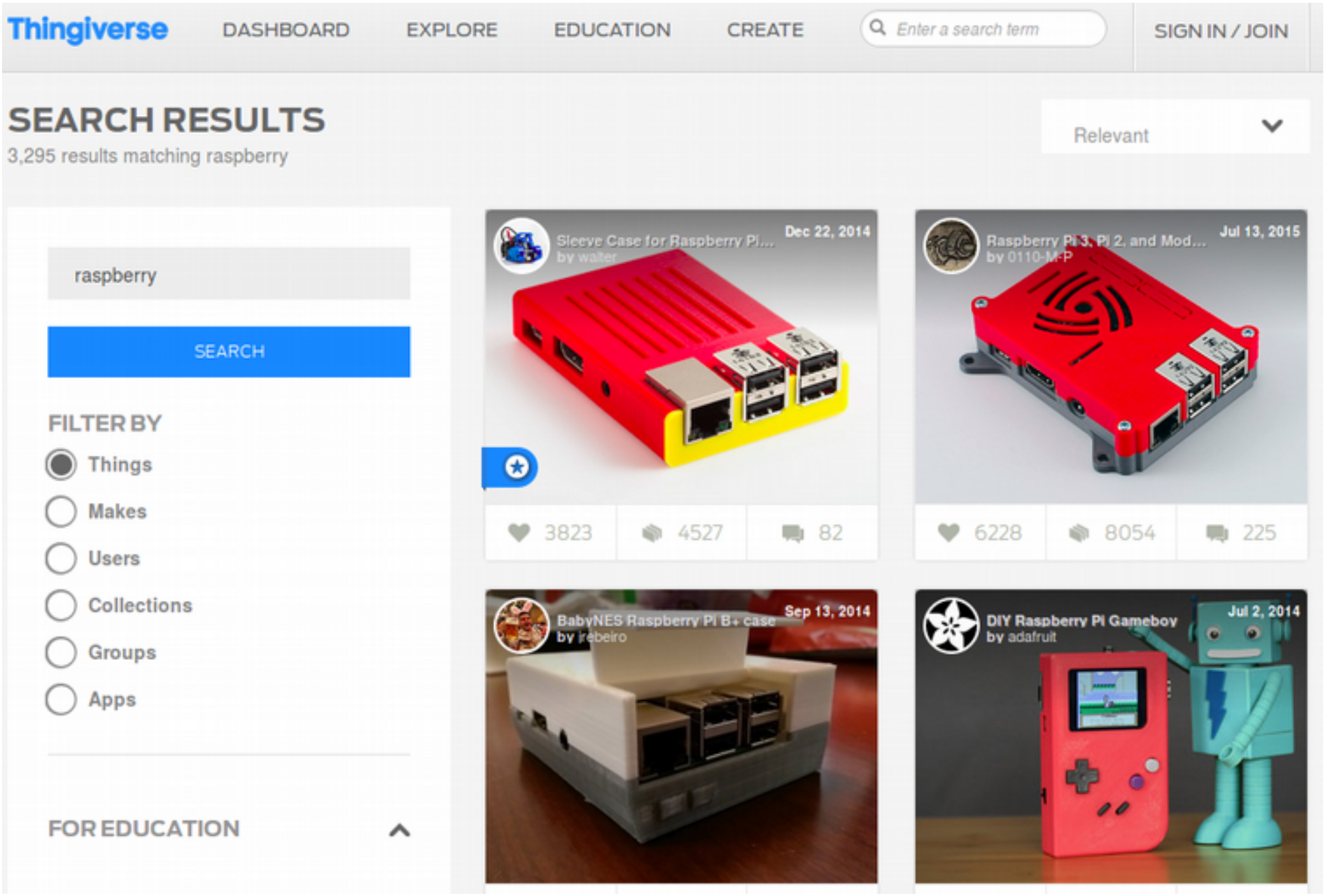
Examples: the Arduino (movement)

The project's products are distributed as open-source hardware and software, which are licensed under the GNU Lesser General Public License (LGPL) or the GNU General Public License (GPL), permitting the manufacture of Arduino boards and software distribution by anyone. Arduino boards are available commercially in preassembled form, or as do-it-yourself kits.





Examples: Thingiverse a.o. 3D print sites



(sidetrack): Linksys WRT54

While it is NOT open hardware, it has had a huge impact on the open movement:

After Linksys was obliged to release source code of the WRT54G's firmware under terms of the GNU General Public License,[37] there have been **many third party projects enhancing that code as well as some entirely new projects using the hardware in these devices.** Three of the most widely used are DD-WRT, Tomato and OpenWrt.

http://www.wi-fiplanet.com/tutorials/article.p[illegible]p/3562391

Food for thought/discussion

/ Free beer and free speech

/ Open business

/ Openness can backfire

/ Limits of openness

/ Openness and security

Free beer and free speech

open is not free as in beer (arduino).

free is not open (your burned windows CD).

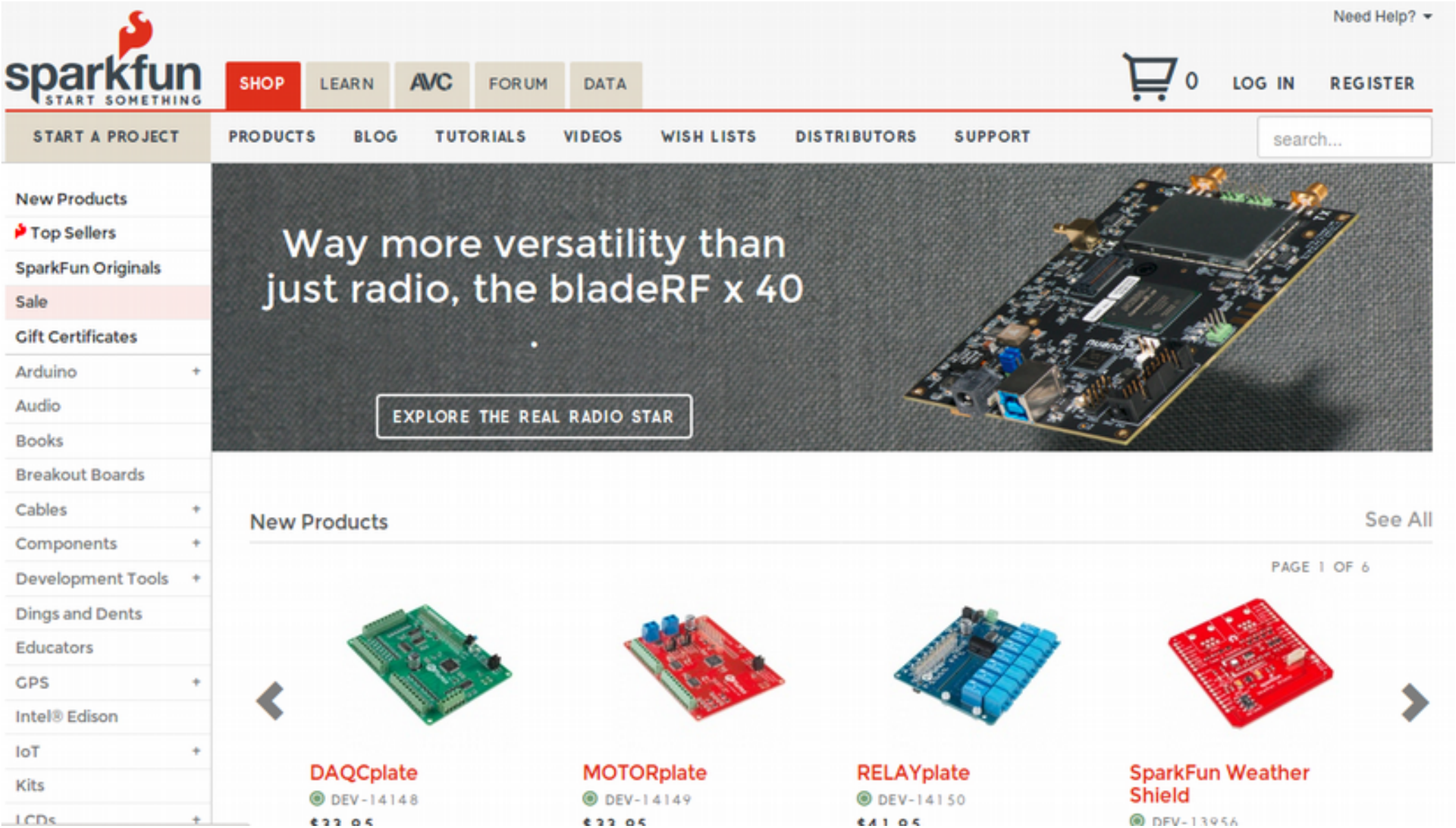
Open business

Openness and making money are not a contradiction.

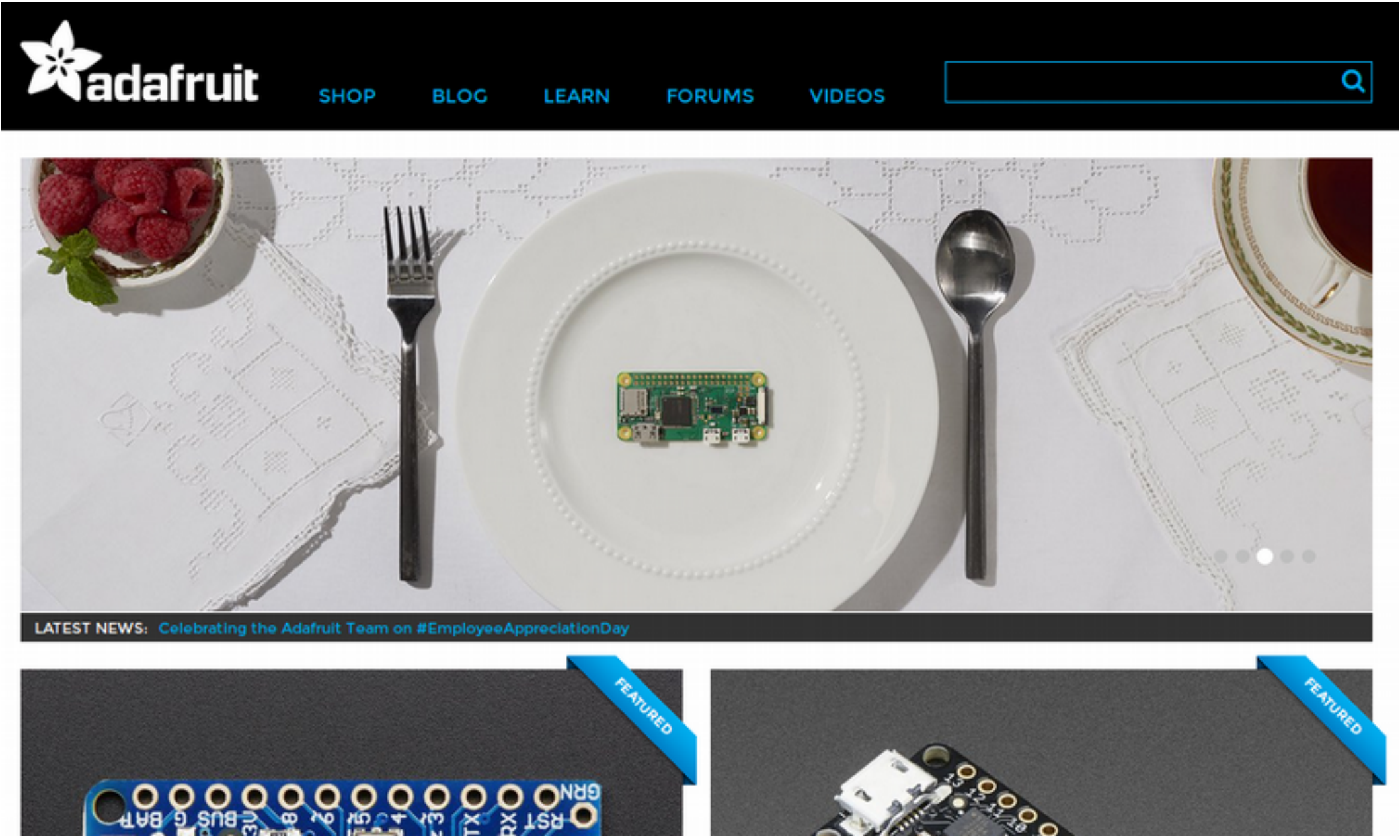
Creating an open technology ecosystem can build and drive your business.

Freemium models, consultancy, shops, workshops, … etc

Open business: Sparkfun



Open business: Adafruit



Openness can backfire

Open licenses give people freedom to run for whatever purpose – including purposes that you dislike.

Openness can backfire

People can and will run
with your designs
and compete
With you

(
Example:
the tangibot
Arduino clones
)

JOSEPH FLAHERTY DESIGN 09.23.12 3:03 PM

CLONING THE MAKERBOT IS LEGAL, BUT DOES THAT MAKE IT RIGHT?

Matt Strong invented a 3-D printer called TangiBot. More precisely, he built an *exact* replica of the MakerBot Replicator and is attempting to raise $500,000 on Kickstarter to fund its production.

IN MOST CASES, he would be met with a swift cease-and-desist letter, but the MakerBot Replicator is open source, meaning anyone can copy it and sell it. While legal, the TangiBot has raised the ethical hackles of many in the maker community.

Limits of openness

Most of our designs contain components that are not open.

Do you know what is inside an IC you are using?

Do you know what is inside your SD card?

What is inside your radio chip?

Limits of openness

Can components be trusted?

Report: NSA Intercepting Laptops Ordered Online, Installing Spyware

Erik Kain, CONTRIBUTOR

I write about video games and science-fiction movies and TV shows. **FULL BIO**

Opinions expressed by Forbes Contributors are their own.

Openness and security

There is no conflict between “open” and “secure” - Many people get this wrong!

On the contrary:

In order to reach high security, you have to be open.
The security of a closed system is impossible to assess. Breaches will not be known.

Openness and digital elections

See for example:

Michael Clouser, Robert Krimmer, Henrik Nore, Carsten Schürmann and Peter Wolf. The Use of Open Source Technology in Elections. International IDEA, 2014.

Citizen Science and Security

Sebastian Büttrich
IT University of Copenhagen
Network Startup Resource Center

ICTP March 2017
ITU.dk
NSRC.org

If you are working with relevant data ...

… then there **will** be conflict, politics …

And attacks.

Internet of Things

“The S in IoT is for Security.”

Some argue that

Surveillance is one of the main motivations behind IoT.

Internet of Things and Surveillance

COMPUTERWORLD

INSIDER

SECURITY IS SEXY

By Darlene Storm, Computerworld | FEB 1, 2016 9:26 AM PT

About

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

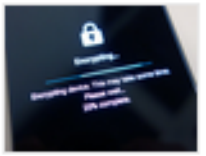
NEWS ANALYSIS

Going dark debunked: Boundless surveillance opportunities via the Internet of Things

Harvard report blows FBI's 'going dark' argument against encryption out of the water as overall surveillance opportunities are brighter than ever thanks to the Internet of Things.

MORE LIKE THIS

Government may tap into your IoT gadgets and use your smart devices to spy on...



Harvard study refutes 'going dark' argument against encryption

IoT security threats and how to handle them

VIDEO

IT security: 3 things you need to know now

Internet of Things and Surveillance

With Internet of Things, FBI In No Danger of Going Dark

February 1, 2016 12:35 by Paul

Internet of Things and Surveillance

techdirt

Techdirt | Wireless News | Innovation | Case Studies | Startups | Net Neutrality | Techdirt Deals!

Main | Submit a Story | RSS

PODCAST Techdirt – When A Typo Breaks The Internet SOUNDCLOUD

<< Congressmen Upton, Walden Latest To Insist... CIA Director Freaks Out After Senator Wyden... >>

(Mis)Uses of Technology
by Tim Cushing
Wed, Feb 10th 2016
8:33am

Intelligence Director James Clapper Warmly Welcomes The Internet Of Things To The NSA's Haystacks

from the *my-god...-it's-full-of-data* dept

The NSA isn't too concerned about the use of encryption. Unlike the FBI, which continues to claim the sky is ~~falling~~ darkening thanks to the spread of math, the NSA is relatively comfortable with the march of technology in this direction.

For one thing, the NSA has made progress towards cracking some forms of encryption. On top of

Internet of Things and Surveillance

BBC Sign In News Sport Weather Shop Earth Travel M

NEWS

Home Video World UK Business Tech Science Magazine Entertainment & Arts

Technology

Amazon resists Echo murder evidence call

23 February 2017 | Technology

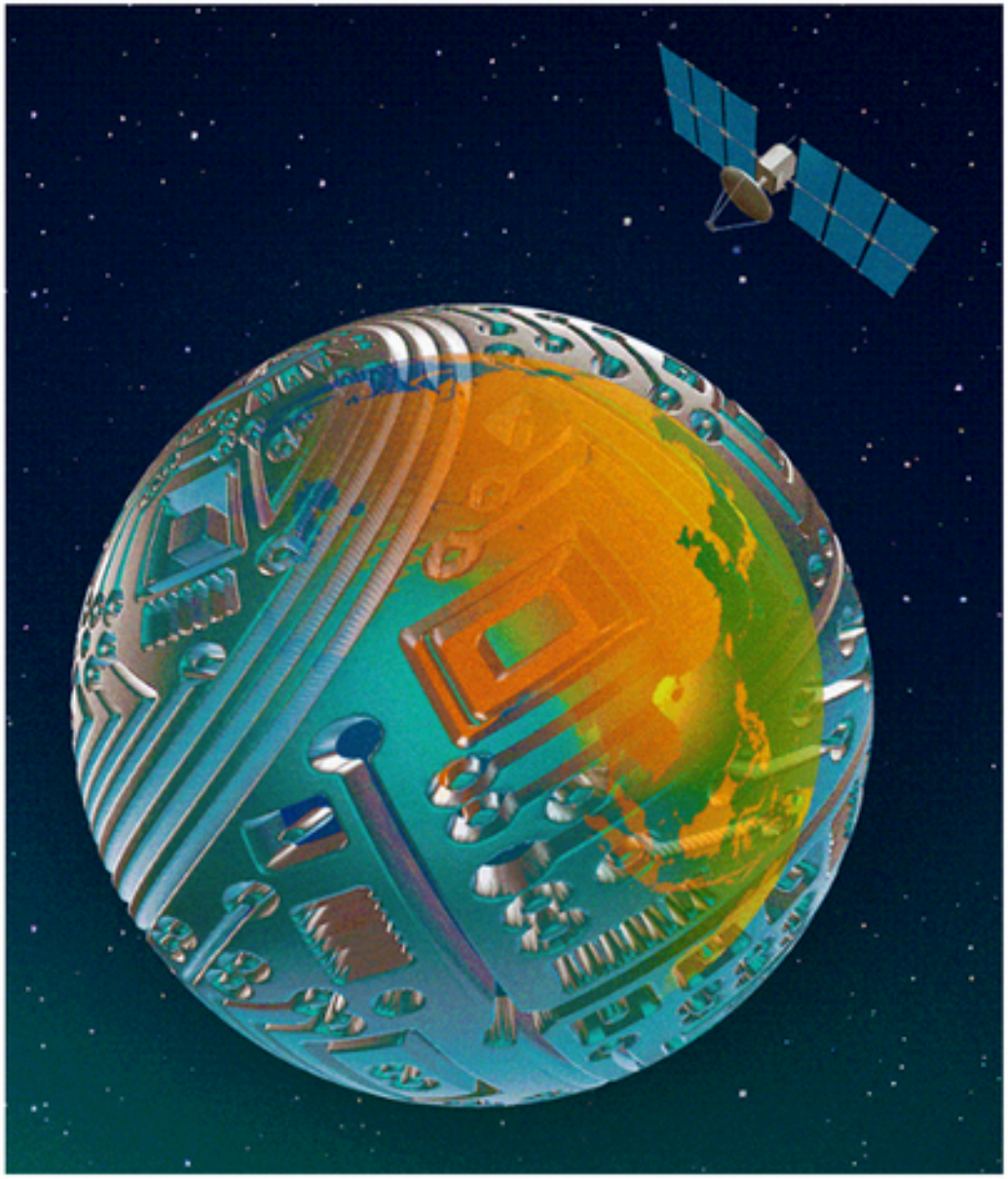
Share

Internet of Things and Surveillance

Click Here to Kill Everyone

With the Internet of Things, we're building a world-size robot. How are we going to control it?

By **Bruce Schneier**



What is Security?

Security in IT and Networks
means
Many (different) things to many different people.

(Bild: Purple Slog, CC BY 2.0)

What is Security? Some Aspects:

Confidentiality

Integrity

Availability

Confidentiality

That data is only seen by those it is intended for.

Integrity

That data is what it is supposed to be,

Only changed by those authorized to,

….

Availability

That networks, data, systems, etc

are available, accessible, ...

Discussion

What are potential threats to

Safecast data?

Environmental data?

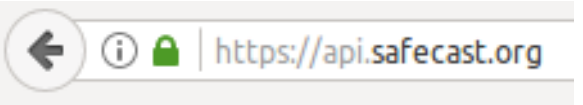
And what can you do about it?

Some (incomplete) advice

Consider online/offline usage.

Technologies used. Openness? Operating systems?

Data communications – encryption.



Moderation/verification of data.

Redundancy of data stores (Mirrors, torrents, ..)

Security of communications

Protection of Networks & systems - Pentesting

NSRC
Network Startup Resource Center

Getting help? There are organizations helping with this.

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

SECURITY WITHOUT BORDERS

Oh, and of course ...

Change the default password.

This is not a joke,
This is not an exercise.

Questions?

Thanks! **sebastian@nsrc.org**