Title: Open Source Sensors: Promoting Access to Knowledge and Data Reliability

Authors: Scott Bulua[1], Puneet Kishor[2], Sonaar Luthra[3], Jason Schultz[4]

Date: January 31, 2015

Acknowledgements: The section on certification includes input from members of the Sensors-Journalism mailing list. Their contribution is gratefully acknowledged.

Interviews were conducted with Sean Bonner of Safecast, and Beth Stauffer from the EPA.

This study is made possible by a generous grant from The Alfred P. Sloan Foundation.

> *Now, while open source really doesn't stop anyone from making a puppy grinder from your open source CNC, I think it's totally fair for the designer to ask you not to do that if you start to go down that path. This is a tricky one because the hardcore licensing people hate to hear this. They think it means the license was weak or something — it's not, it's a strength that we're a community who can talk to each other when needed.*
>
> - Phil Torone, The {Unspoken} Rules of Open Source Hardware[5]

---

1. NYU Law
2. Creative Commons
3. Water Canary
4. NYU Law
5. Torone, Phil, "The {Unspoken} Rules of Open Source Hardware," February 2, 2012, MAKE Magazine Blog: http://makezine.com/2012/02/14/soapbox-the-unspoken-rules-of-open-source-hardware/

Table of Contents

(i) Introduction

This paper maps the challenges and opportunities presented by the rise of sophisticated and inexpensive sensing technologies and their intersection with efforts to make technology "open." In this instance, openness denotes three general areas that take on new meaning in the context of sensors: knowledge (how they work, how they are made, how they perform and how their limitations can be surmounted), accessibility (how one gains access to the physical sensor itself, how one acquires the rights to produce and manufacture sensors), and stability (how reliable, precise, accurate, consistent are the data they produce, and what biases they introduce).

After an overview of the current state of sensors, including the process of sensor development, we examine the risks that closed development presents both to the greater public and manufacturers, the shortcomings of existing models for open development, and end with suggestions for new legal and institutional frameworks to support open sensor development.

(ii) The Current State of Sensor Technology and the Sensor Development Process

The term sensor can denote many different types of electronic components, scientific instruments, or monitoring devices that measure physical, chemical or biological phenomena and translate them into electrical signals. What distinguishes them from other instruments of measurement is that the electrical signals they output can be read and processed by computers. Data collection and data entry are usually separate steps, but sensors make it possible to automate this process, and to even automate a given response (turning up a heater, for example) when specified conditions are met. This offers the benefit of speed and efficiency, allowing a user–or a program–to move from question to answer to action without delay. This is another

reason why sensors defy traditional categories of hardware, software and datasets: they erode these boundaries.

As we shall see, sensors may need to be treated as a different category altogether. It may be necessary to rethink openness in frameworks outside of the historically-siloed development of intellectual property licensing practices as sector or technology specific. This may even require embracing processes that enact restrictions, regulations and certifications – tools that would seem antithetical to open culture, but may eventually prove to solidify its foundations in the sensor space.

(iii) The Map Is Not The Territory

Taking a photograph used to require manually focusing a lens, estimating how much light to expose onto celluloid film and for how long, using chemical reagents to fix negative images onto the film, shining light through negatives to expose photo-paper, and using chemicals to develop the images on paper. It also meant having to repeat multiple steps to achieve a desired result, maintaining a dark room, owning very specialized equipment, and recurring expenses each time a photo was taken or developed. In other words, it was as complex and resource-intensive as any specialized task performed by scientists in a lab.

All of these rules have changed with the rise of digital photography: photos are captured with the press of a button, it costs virtually nothing to take additional photographs, results are instantaneous, and the cost of all the essential equipment is now less than what it once cost to develop a single roll of film. It also means that we can safely assume that any event of social or political significance anywhere on earth will be photographed, and that normal citizens can perform roles that were once reserved for journalists and photographers.

This is what makes sensing technologies powerful: they automate complex processes and methods of data collection and they carry the potential to monitor real-world phenomena at unprecedented speeds and scales. In spite of all of these technical breakthroughs, the limitations of the sensors used in commercial digital cameras are not widely understood.[6] For instance, *no commercial light sensor available today is capable of directly measuring color*. In today's photodiodes, CCD's, CMOS's, NMOS's, photomultiplier tubes, and all other photon-based optical sensors the sensing element is only capable of measuring the intensity of light, and frequency (or color) is estimated through indirect means.

In photography, the established method for getting around this borrows another property of light used in color display technology: one can produce most visible colors by mixing together different amounts of red, green and blue light (e.g. mixing together the light emitted by a green LED and a red LED can produce almost any shade of yellow or orange). Instead of measuring color itself, each pixel of a digital camera's sensor is covered by red, green or blue filters on top of each pixel in an image sensor. Although the three-channel RGB method allows cameras to capture full-color images, it does not measure color accurately. This is why it can be so difficult to capture flesh tones, and why "natural-looking" images often require exaggerated lighting schemes or digital post-production. These limitations of the sensing technology have existed since the birth of color photography,[7] yet they are taking on new significance in an age where the

---

6. A much more in depth account of what follows on imaging, the drawbacks of commercial sensors, and more accurate sensing paradigms can be learned from Water Canary Senior Scientist, Eric Rosenthal's 2004 Paper, "Waves vs Photons," http://www.creative-technology.net/Papers/Peer%20review%20paper.pdf

7. The first permanent color photograph was taken in 1861 by Herbert Maxwell, a pioneer of the additive RGB method. He took three different photographs of the same scene using red green and blue filters, and then reversed the process by projecting each image through its respective filter so that they combined to produce a full-color image.

information collected by sensors is routinely mined for data, and automated control systems are being programmed to make decisions based on sensor data with a growing level of autonomy.

RGB images are not the same as what we see. They consist of a biased approximation of the color space they capture. Yet if a programmer fails to understand this, any statistical analysis applied to computer vision has potential to find patterns in data that do not exist. Even if a programmer does understand these tradeoffs, the specific wavelengths of red, green and blue used in filtration can vary between manufacturers at statistically significant levels (and in rare cases even vary at across specific product lines) that cannot be accurately accounted for in an algorithm without a tested calibration of each sensor.[8]

It is one thing for artifacts to limit the applications of computer vision in the realm of input devices, as with computer interfaces and video game controllers, especially if their imprecision does not interfere with the overall functionality of the system. But in the case of a self-driving car, a drone, a scientific robot or an environmental monitoring device, misunderstanding the limitations of a sensor could have potentially grave consequences.

For instance, Google's unreleased self driving car is unable to identify the color of traffic lights when its cameras are in bright sunlight,[9] it is not able to drive on 99% of US roads, it cannot tell the difference between rain and snow, and a widely held public belief that the core

---

8. see Alvin G. Wee, Delwin T. Lindsey, Shanglun Kuo, William M. Johnston, "Color accuracy of commercial digital cameras for use in dentistry," Dental Materials Vol. 22 (6) pp. 553-559. RGB is considered to be a "device dependent" color model. For a high level overview of commercial devices this post may be worth reading: http://www.extremetech.com/extreme/49040-different-devices-use-different-color-models

9. http://www.nydailynews.com/autos/google-self-driving-car-article-1.1924691

technical issues have been resolved has academics, engineers and researchers concerned.[10] [11] To Google's credit, each of the limitations listed above were disclosed voluntarily by the team itself this past summer, and director Chris Urmson's public statements have indicated the car is at least five years away from production.[12] Such transparency is admirable, given the cultural shift that autonomous vehicles promise and the many potential risks they present to public safety.

But it is not a given that companies engaged in developing sensor-based technologies will follow suit. As with any high-risk, resource-intensive endeavor, it is not often in a company's best interest to share the limitations of its products. Even though regulations exist to protect public safety and consumers from fraud, countless automotive and pharmaceutical recalls[13] have demonstrated that our systems of regulation are far from perfect, and often struggle to keep pace with technologies that defy classification.

On one hand, the lack of appropriate regulations and testing requirements means that some vendors may choose to exaggerate the performance of their products, or selectively hide data that undermines confidence in their performance. On the other hand, the need to assure consumer confidence also carries with it the risk that manufacturers will choose to simply collect more detailed information than may be necessary to reach a given benchmark, a topic of already growing concern with respect web advertising platforms and government surveillance. If, for

---

10. http://www.technologyreview.com/news/530276/hidden-obstacles-for-googles-self-driving-cars/; http://www.theatlantic.com/technology/archive/2014/05/all-the-world-a-track-the-trick-that-makes-googles-self-driving-cars-work/370871/

11. Preliminary polling has shown that 75% of Americans are ready to purchase Google's car once it is available: http://www.usatoday.com/story/money/cars/2014/07/28/driverless-self-driving-cars-poll-insurancecom/13277937/

12. http://www.nydailynews.com/autos/google-self-driving-car-article-1.1924691

13. For instance: http://www.nytimes.com/2012/07/03/business/glaxosmithkline-agrees-to-pay-3-billion-in-fraud-settlement.html?pagewanted=all

instance, Google were to develop and deploy a true full-spectrum camera with an advanced dynamic range capable of measuring color without filtration, it might immediately find all the data necessary to successfully navigate any scenario it might encounter. But such a camera would also be capable of fueling advanced facial recognition capabilities, identifying individuals in crowds with high temperatures, or performing countless other measurements that have been the subject of controversy in airport security. These are not issues that concern most people or programs in daily life, but they do concern scientists, engineers, civil liberties advocates, and every field concerned with protecting public health and safety.

Each of these areas has historically required a great deal of regulation and oversight. Sensors will not change that, but they will require a shift in how this regulation and oversight is performed that will require deep technical knowledge, and a renewed attention to methods that establish trust in scientific research.

(iv) Trust in Science

Reproducibility and repeatability are fundamental standards used to test scientific claims and theories. When enough members of a peer community verify a finding, it gains scientific merit. To this extent, science is an "open" discipline that frowns upon secrecy and anything that obstructs this process of peer review.

In spite of this, transparency in science has material constraints that limit the size and composition of peer groups:

i. **Training**: Is one qualified to evaluate the work?

ii. **Accessibility**: Can one access the paper/finding?

iii. **Resources**: Does one have the tools/resources/facilities to examine the findings and/or present alternative and competing theories?

These constraints determine who participates in science. In ideal circumstances they promote trust by excluding factors that might compromise or contaminate the integrity of experiments. For instance, the staffing, safety and maintenance requirements at an EPA-certified laboratory, help to ensure that work is performed in controlled conditions, with properly calibrated equipment by people who use the same methods. This ensures that fewer errors and miscommunications take place. Yet when these constraints eliminate too many people they can produce circumstances where critical issues are ignored, conclusions reinforce entrenched biases, there is too little accountability, or very little transparency.

Science requires objectivity and, for better or worse, exclusivity. This places a limit on who can participate, but that limitation can be overcome through the use of technology and breaking down complex processes into more easily managed parts. Today these parts generally break down as follows:

i. **Measurement Standard** - An agreed upon metric for quantifying a given phenomenon that will be investigated.

ii. **Device/Instrument Accuracy** - An instrument for performing measurements in accordance with a measurement standard that has a verifiable sensitivity level and a quantified margin of error.

iii. **Methodology** - A protocol for performing measurements using agreed upon standards and trusted instruments that helps to minimize operator error and promote consistent practices among different practitioners

iv. **Technical training** - An individual that has been taught to perform measurements in accordance with a prescribed methodology.

v. **Facility certification and maintenance** - An agreed upon environment under which work can be performed under controlled conditions, and a method for ensuring facilities continue to comply with the requirements of such an environment.

vi. **Peer Review** - A process whereby experts analyze the work performed and the claims it supports to identify errors and external variables that may have biased results.

Today it is possible to integrate these steps into sensor enabled hardware, as with home blood-glucose meters used by diabetics. Given a sensor designed in accordance with a measurement standard that is certified to perform within a specified margin of error, methodology can be mapped onto a device's firmware, technical training can be coded into an interface that automatically performs any selected subroutine, additional integrity sensors can be applied to verify proper environmental conditions, and the error identification goals of peer review can be accomplished through redundant data collection efforts. This does not eliminate the need for scientific expertise altogether, it rather focuses it upon research and development so that a perfected device performing to

specification can be used by non-experts to perform very complex tasks with less resources. Reaching this goal, however, is no simple task.

(v) Challenges facing sensors today

The use of sensors in consumer electronics has exploded in recent years, yet sensors face major scalability issues today that - relative to conventional electronic components - result in slow development cycles, slow adoption rates, low efficiency, platform/system validation burdens for hardware developers, and very complex sourcing processes.[14]

Some of these challenges reflect a shift away from the traditional model where commercial end-products are made exclusively by the sensor manufacturer, placing all the burden, and all the reward, on the manufacturer's ability to create a reliable system of measurement, to market a compelling application of that system of measurement, and to sell them in volumes that justified their investment. Warren S. Johnson's electric thermostat, widely regarded as the first commercial sensor, was patented in 1883, enabled the founding of Johnson Controls in 1885, a company that launched the building control industry. In the 1940's Samuel Bagno developed the first motion sensors and brought to market the first ultrasonic alarm over the next decade.

Although many companies – especially those that build original scientific instrumentation or medical devices – still pursue a similar strategy, what has fundamentally changed in the decades since, is that one can now purchase a third-party sensor and integrate it into an original product without taking on the risk of sensor development. This carries the promise of promoting more data collection in more devices by more people. Yet, from a development standpoint, this

14. IEEE Std 2700-2014 at 9.

means that the institutional knowledge of the sensor manufacturer has to be transferred as efficiently as possible from original equipment manufacturers (OEM's) to end-product manufacturers to overcome integration challenges.

This process has been riddled with challenges due to the high cost of sensor testing, and the lack of industry standards that allow for direct comparisons between different sensors. The Microelectromechanical Systems Industry Group (MIG) estimates that OEM's spend up two thirds of the total cost of sensor manufacturing on sensor testing. This is expensive, and it is compounded by the need for customers (for instance mobile device manufacturers) to develop their own system for verifying and evaluating sensors with different specifications.

Despite early efforts to standardize motion sensor parameters, it is only in 2014 that the IEEE has introduced the first industry standards for specifying commercial sensor performance.[15]The recently published "IEEE Standard for Sensor Performance Parameter Definitions" covers the eight most common sensors used in consumer electronics today: accelerometers, magnetometers, gyrometers, pressure sensors, humidity sensors, temperature sensors, ambient light sensors, and proximity sensors. Many of the parameters described have been present on sensor data sheets for years, but there has been a lack of third-party standards and little consensus on units of measurement. Although each sensor requires unique parameters to characterize the phenomenon it measures, key issues that must be taken into consideration for any sensor include but are not limited to:

- the sensor's precision/sensitivity
- the sensor's accuracy/sensitivity error

15. Id.

- signal-to-noise ratios
- dynamic range of sensitivity
- bias/drift in accuracy or precision due to changes in temperature
- output errors due to off-axis or misaligned inputs
- how long until the sensor is ready to perform a measurement
- how long it takes to transition between measurements

Any ambiguity about how each of these issues should be defined and measured makes it difficult for OEM's to market competing sensors in established categories, makes it harder for other manufacturers to evaluate and source sensors, increases the time it takes for products to reach the market (TTM), and increases the likelihood that a device will not produce accurate, consistent or reliable data.

These are major challenges that mainly concern engineers, and there are established channels today for addressing them within traditional disciplines. But these channels are far from efficient, and do not yet take into consideration the downstream impact of manufacturing and testing practices on datasets.

(vi) The Risks of Closure and The Promise of Openness

i. Risks of Closure

It is generally the task of scientists to establish the credibility of methods for detecting physical, chemical and biological phenomena, the task of engineers to standardize this method into a replicable apparatus that can be commercialized, and the task of industry alliances to find common ground and ensure interoperability and reliability of new classes of products.

Finding common ground is a relatively simple task for industries in the case of traditional electrical devices and components - a standardized set of tools like a multimeter, oscilloscope, or spectrum analyzer, combined with trustworthy data sheets on components are sufficient for most diagnostics that an Electrical Engineer performs daily. Yet every sensing paradigm is different and requires its own system for assessing performance (i.e. an accelerometer and a humidity sensor require different evaluation methods). In some areas, like imaging, commercial camera sensor manufacturers benefit from practices already developed in areas of optics where highly precise scientific measurements are necessary. As long as there is a more precise instrument available to measure against, developing a new sensor, or evaluating a 3rd party sensor for integration into a more elaborate device, is much more straightforward. Even in a highly regulated space, like medical devices, getting approval for sensor-based consumer devices (like blood glucose meters) is far less complex if the method of detection has already been proven and approved by the FDA for use in medical settings.[16] Yet because every sensing paradigm is different and requires its own system for assessing performance (i.e. an accelerometer and a humidity sensor require different evaluation methods), this agreement is largely absent today, and necessitates redundant evaluation efforts at every level of development. In areas where a sensing paradigm has not yet been established - or an evaluation practice has not been endorsed by a larger community - agreement is largely absent today. That calls into question when and how data can be trusted, and it necessitates redundant evaluation efforts at every level of development.

16. A well established route towards FDA approval of a device is to prove a substantial equivalent to an existing approved device.

Today this presents a serious problem for anyone seeking to collect and aggregate data from distributed sensors, because it means that *even consumers* must engage in redundant assessments of sensor integrity/consistency. This means that there are hundreds of inexpensive air quality sensors on the market today that appear to be substantial equivalents to more expensive devices, but different sensors at the same location - even those unofficially endorsed for citizen science applications by the EPA - may consistently report different levels of the same contaminant.[17] Even in a circumstance where a single sensor or device has been agreed upon by a community, there remain calibration challenges that can limit the reliability of any system.

Each of these areas presents a possible point of failure in a data collection effort, yet in the absence of shared parameters, metrics, resources, methods, practices, designs, and - optimally - patents, there are no efficient ways for OEM's, vendors, engineers, scientists, hackers, athletes, makers, sensor journalists, or citizen scientists to account for the factors that threaten data integrity. Although these challenges are unique to sensors, there do exist collaborative processes for tackling problems in open development communities that are well established and worthy of consideration.

Sensors may not map directly onto the dynamics at play in Open Software & Open Hardware, and data integrity may require engagement with legal frameworks outside of patents and copyright. What follows outlines the current state of each of areas in an effort to identify

17. Source: Interview with Sean Bonner of Safecast on 9/5/14 - a global open source radiation data collection community - commenting on their initial experiments with air quality sensing. Safecast's open source geiger counter makes use of a global standard vacuum tube that generates discrete electrical pulses every time a radioactive particle passes through it. This digital sensor directly measures the phenomenon in question and requires no calibration. In stark contrast, today's air quality sensors often use different detection methods that are sensitive in different ways, making calibration and sensor evaluation a much more complicated task.

how a paradigm like Open Sensors might be established through creative use of existing legal, contractual and organizational frameworks.

ii. The Promise of Openness

Intellectual Property Law and the Legal Mechanisms for Protecting Open Development

Intellectual property law serves as the basic tool to protect the output of open communities, including the open hardware and open source software communities. For instance, while the copyrighting software has been criticized for stifling innovation,18 it has also been a necessary condition for the development of a robust community of innovation around software. Open source software licenses work because they harness rights granted by the copyright law to tie the developer's desired restrictions to a license to use and modify the source code of their software. By imposing conditions, software engineers can rely on legal remedies in federal courts – and perhaps more importantly, the threat of legal remedies to force compliance with community norms.

The use of IP law protects the reliance interests of contributors to open projects. Initially, engineers who contribute to a project want to rely on the fact that they can use the software subsequently, and can continue to modify and improve it; this is at the heart of all open source licenses, as well as the Open Source Definition.[19] The GNU General Public License, the most widely used open source software license,[20] grants the following: "You may modify your copy or

18. See, e.g. Pamela Samuelson et. al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 Colum. L. Rev. 2308, 2429 (1994) (finding that "[e]xisting legal regimes have, however, found it difficult to recognize and deal appropriately with other characteristics of computer programs.").

19. See *Open Source Definition*, supra note 10.

20. *Top 20 Open Source Licenses*, Black Duck Software Resource Center, http://www.blackducksoftware.com/resources/data/top-20-open-source-licenses (last visited May 1, 2014).

copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications."[21] These broad rights allow other engineers to integrate open source software into custom software applications, for personal or commercial use. Furthermore, engineers want to ensure that the skills they develop, and the intimacy with a particular software product, can be transferable as they move between projects and employers. By open sourcing a project instead of keeping it as a trade secret, an engineer is able to rely on the fact that they will be able to continue using their work.[22]

A major fear driving open source software licenses, particularly copyleft licenses such as the GPL, is that software will be co-opted and trapped by a corporation, who will profit from that software, without monetary compensation to the developers and without contributing its improvements back to the community. These concerns have already been apparent in the world of open hardware,[23] and licensing solutions attempt to prevent this outcome. The Open Compute Project, for example, will allow contributors to license their hardware projects either under a permissive license, or under a restrictive license that requires that modifications, if used in a production environment, be made publicly available and accompany distributed hardware.[24]

---

21. *GNU General Public License, version 2*, GNU Operating System, http://www.gnu.org/licenses/gpl-2.0.html (last visited May 1, 2014).

22. While mobility might seem detrimental for employers, it has large positive externalities. See, e.g. Bruce Fallick et. al., *Job-Hopping in Silicon Valley: Some Evidence Concerning the Micro-Foundations of a High Technology Cluster*, available at http://www.federalreserve.gov/pubs/feds/2005/200511/200511pap.pdf (finding that "frequent job-hopping facilitates the rapid reallocation of resources towards firms with the best innovations" but also reduced incentives to invest in human capital.)

23. See *Brief History of Open Source Hardware Organizations and Definitions*, supra note 2 ("In 2005, TAPR began working with one such group, which was developing high performance software defined radio products and wanted to contribute their free time and expertise to the ham radio community. The group feared that their efforts might be co-opted by commercial entities and therefore asked for TAPR's assistance in developing a license to achieve their goals.") (citations omitted).

24. See *Request for Comment*, supra note 29.

(vii) The shortcomings of existing "Open Source hardware" licenses

In light of the success of the free and open source software movement, many thoughtful engineers and attorneys have attempted to take the model of open source software licensing and "port" it to hardware. Since sensors combine hardware, software, and data collection, one can see the compelling case for such importation. However, key differences exist in how sensors function, both individually and as part of larger networks, that leave the open source software licensing model coming up short in terms of achieving the openness that a successful long-term effort at creating a commons is likely to require.

(viii) The Collaborative Product and Hardware Documentation Licenses

This section introduces the idea of "collaborative product", which is separate from the physical end-product yet contains all of the elements necessary to collaborate, and can be used to effectively recreate the physical object with reasonable effort. Hardware documentation is the locus of collaboration since it allows engineers to collaborate on electronics designs.

In software, source code and associated documentation files are clearly the collaborative products.[25] Since individual programmers have the basic tools they need to turn source code into a usable application (e.g. operating systems, code editors, and compilers), only the source code must be shared in order for software engineers to view each others' work, make modifications, and collaborate on a software project. In contrast, the executable file, which is the object code

25. Source code files are typically the sole medium for collaboration. On Github, among the most popular repositories, over 5 million people collaborate on source code. *About*, Github, https://github.com/about (last visited May 1, 2014).

file that a computer is able to run, is not the collaborative product, and is generally not shared among participants in an open innovation community.[26]

In open hardware, the documentation files serve a similar purpose. Whether HDL code, schematic layouts, layout files, CAD files showing the physical design of casing, or written documentation showing the physical design of a final product that uses off-the-shelf components, these human-readable files allow hardware designers to work together and improve other products, prior to manufacturing. This idea is validated by the emergence of companies who seek to allow collaboration in hardware design, in attempt to replicate the efficiency gains of open source software. These products, such as Upverter and Knowable, allow engineers to collaborate on schematic diagrams and circuit board layouts.[27] The availability of software-based hardware simulators enables engineers to test parts of their hardware on a computer before starting the manufacturing process.[28] This allows engineers to test their collaborative product without creating a physical embodiment. As production tools available to open hardware engineers become more complicated, we can imagine that more work will be done by robots and less done by human hands; at that point, documentation is surely the collaborative product to the extent it

---

26. While some projects provide development or stable builds, engineers are encouraged and expected to compile their own applications from source code. Several applications have been developed to assist users in compiling open source applications. See, e.g. Homebrew: The missing package manager for OS X, http://brew.sh/ (last visited May 1, 2014).

27. See Upverter, https://upverter.com/ (last visited May 1, 2014) (“Upverter is a launchpad for engineers to turn their ideas into products. When it becomes easier to build hardware, radical innovations will result not only in hardware, but in how we solve for the world of tomorrow.”); Knowable, http://knowable.org/ (last visited May 1, 2014) (“Knowable is a place that enables you to join forces with like-minded Makers. A place that let's you organize your files, tasks and team members in order to get your next idea ready for market as fast as possible.”).

28. Simulators primarily work for integrated circuits that are designed with HDLs and CAD tools. See Horowitz, supra note 13, at 908.

instructs the robotic assembler to manufacture a hardware product, as a compiler assembles a finished software product today.

Several licensing options have been proposed to reconcile the differences between software protection, where copyright clearly applies, and hardware protection, where IP protection is more complicated.

i. TAPR

Tucson Amateur Packet Radio Open Hardware License (TAPR OHL) is a license that combines copyright and contract principles, and licenses rights under patent and copyright. TAPR begins with a "Preamble", a useful manifesto about the goals of the license and its legal theory. This manifesto supports the role of the license as "internal law" as much as it is judicially-enforceable external law.

One flaw of the TAPR OHL is that it is targeted towards electronics hobbyists, rather than engineers creating widely-used hardware. Since TAPR itself is a group that creates hobbyist radios, this is a good fit for the client, but it does not make for a widely-applicable license. This is reflected by the license's decision not to consider HDL to be documentation, and to exclude it from the scope of the license (presumably to be covered by a separate software license like the GPL).

Another issue with its contract-based approach is that contracts are between two parties. The license states: "By (a) using, copying, modifying, or distributing the Documentation, or (b) making or having Products made or distributing them, you accept this Agreement." However, many of the rights granted are not otherwise protectable, for example the right to distribute products. For distributors, agreeing to this contract would restrict their rights, whereas refusing

the contract would not prevent them for distributing the products. Therefore, there is a clear license circumvention method, and an incentive to circumvent.

ii. CERN OHL

The European Organization for Nuclear Research Open Hardware License (CERN OHL) is a license focused on open science and was created in conjunction with CERN's Open Hardware Repository.[29] The license seeks to cover both the documentation and final products,[30] thus forming a license to both patent and copyright rights held by the licensor. The CERN OHL is a "copyleft" license, and requires that any modifications to documentation are made public. However, the CERN OHL states, "Licensor shall not assert his rights under the foregoing proviso unless or until a Product is distributed,"[31] so internal use and testing do not introduce obligations. The license also has a strict attribution requirement, and requires the distribution of documentation, or a means of accessing the documentation, with any end product.[32]

While the CERN OHL makes reference to various activities, such as reproduction and distribution of documentation, and the manufacture and use of products, it does not specifically refer to copyright or patent as bodies of law. This lack of clarity about what exactly is being licensed is detrimental to the goal of clarity, and the license's ultimate enforceability. At the same time, it might make it more adaptable to legal regimes with different intellectual property concepts.

---

29. *Supra* note 46.

30. CERN OHL, supra note 6, at §2.1.

31. CERN OHL at §3.3.

32. CERN OHL at §4.1.

iii. Solderpad License

The Solderpad License is a straightforward modification of the Apache License, a common open source license originally intended for software, that attempts to incorporate more rights so that documentation and physical products can both be covered under a single license.[33] By appropriating Apache rather than starting from scratch, the creator of the Solderpad License is attempting to migrate the norms of the Apache Foundation and project to the hardware community.[34] The license grants rights under "copyright and any similar right including design right (whether registered or unregistered), semiconductor topography (mask) rights and database rights (but excluding Patents and Trademarks)," and contains a patent license from each contributor to any claims that are necessarily infringed by the greater work.

Working from an existing license, unlike CERN and TAPR, is an excellent strategy from a norm perspective. However, the license's reliance on the defined terms "source" and "object" form, rather than referring to documentation and physical products more directly, makes the license less directly suited to the hardware development process, and more suited to being a generally applicable and permissive "open" license.

OSHWA Definition

http://www.oshwa.org/definition/

---

33. Andrew Katz, Re: the solderpad hardware license, OH Updates, http://lists.openhardwaresummit.org/pipermail/updates-openhardwaresummit.org/2012-March/000796.html (last visited May 1, 2014) (nothing that "[t]he Solderpad licence addresses these issues explicitly, and avoids a situation where you choose Apache or BSD for documents (and the hardware itself) which do not have these other rights, and another more explicit licence for circumstances where it does.").

34. Andrew Katz, Re: the solderpad hardware license, OH Updates, http://lists.openhardwaresummit.org/pipermail/updates-openhardwaresummit.org/2012-March/000806.html (last visited May 1, 2014) ("That's one reason why I felt Apache was a good starting point, as Apache is not only a well understood licence, but the norms attaching to the Apache community are well understood, including the way in which the community interacts with traditionally structured commercial entities.").

The most prominent definition of open hardware is that provided by the Open Source Hardware Association ("OSHWA") in the form of the current OSHWA definition:[35]

> Open source hardware is hardware whose design is made publicly available so that anyone can study, modify, distribute, make, and sell the design or hardware based on that design. The hardware's source, the design from which it is made, is available in the preferred format for making modifications to it. Ideally, open source hardware uses readily-available components and materials, standard processes, open infrastructure, unrestricted content, and open-source design tools to maximize the ability of individuals to make and use hardware. Open source hardware gives people the freedom to control their technology while sharing knowledge and encouraging commerce through the open exchange of designs.[36]

This definition encapsulates several concepts related to freedom: freely available to build and study, free of cost to users and manufacturers, and freedom to modify and tinker. The concept of open hardware is slightly more complex to understand than the corresponding concept of open source software, which might contribute to its lack of success. Software is embodied exclusively in source code, and its product, generally an executable file, can be created from the

---

35. The OSHWA definition is modeled on the Open Source Definition promulgated by the Open Source Initiative. The Open Source Definition, Open Source Initiative, http://opensource.org/osd (last visited May 1, 2014).

36. Definition (English), Open Source Hardware Association, http://www.oshwa.org/definition/ (last visited May 1, 2014).

source code with minimal skill and cost. In contrast, hardware is embodied in code and documentation encompassing several forms, and creation of a final product might require the use of expensive and complex machinery, materials, and components.

(ix) Possible Legal Frameworks for Protecting Open Sensors

i. Copyright in circuits

One possibility for protecting open hardware designs would be to assert copyright in circuit design, and enforce restrictions through a copyright license. No court in the United States has considered the question of copyrightability of a physical PCB. There is a strong chance that a circuit board would be held to be a copyrightable work,[37] although such protection would likely be thin,[38] because the primary purpose of a PCB is functional. Still, the author of a circuit board design might be able to enforce their copyright against another party who made an exact copy of a board's structure and layout.

The history of the Semiconductor Chip Protection Act suggests that PCBs are not protectable in their physical manifestation. In the congressional hearings leading to the passage of the Act, the Copyright Office told Congress that it had refused attempts to register circuit boards and semiconductor chips "because no separate artistic aspects had been demonstrated."[39]

---

37. Ackermann, supra note 15, at 204 ("Given that the arrangement of components and wiring traces on a printed circuit board is subject to personal choices on the part of the designer, it is reasonable to argue that the circuit board is a work subject to copyright, but as with most of the outputs of the design process, that copyright is likely to be weak.")

38. Micah D. Stolowitz , Re: Circuit Board Designs, CNI-Copyright E-mail List (Apr. 17, 1996. 10:17 AM), http://www3.wcl.american.edu/cni/9604/8939.html (arguing that "THIN protection, i.e. a literal, exact copy of a PCB or ASIC layout should be infringement.")

39. Brooktree Corp. v. Adv. Micro Devices, Inc., 977 F.2d 1555, 1562 (Fed. Cir. 1992), citing Copyright Protection for Semiconductor Chips: Hearings on H.R. 1028 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary, 98th Cong., 1st Sess., 77 (1983) (statement of Dorothy Schrader, Associate Register of Copyrights for Legal Affairs).

These attempts were made by Intel to copyright semiconductor designs, and Intel initially sued the Copyright Office to compel registration, but then ceased its suit and decided to pursue a legislative strategy instead.[40] As a result, we do not have any conclusive guidance on the copyrightability of circuit boards, although an engineer might be successful in demonstrating protectability if they could show creative elements in circuit design that are not purely functional.

ii. Copyright in Data

It is generally accepted that data resulting from scientific research cannot itself be copyrighted. However, the sequence, structure, and organization of data might be copyrightable. This could apply to data sets, e.g. the data used to train or test sensors, when organized in a manner that displays a "modicum of creativity".

iii. Patent Licenses

The role of patents

Hardware and the processes used to manufacture hardware are functional, and thus implicate utility patents. Patents do not protect entire hardware products themselves, but can protect a process or machine if it is novel, useful, and non-obvious, and falls within the subject matter of the patent system.[41] These requirements, particularly the non-obviousness and novelty requirements, would rule out many open hardware projects, which seek to provide open alternatives to commercially available products. However, some hardware projects, particularly those with innovative sensor designs, are likely to produce patentable inventions.

---

40. For more background, see Leo J. Raskind & Richard H. Stern, Symposium: The Semiconductor Chip Protection Act of 1984 and its Lessons: Introduction, 70 Minn. L. Rev. 263 (1985).

41. 35 U.S.C. § 101 (2013).

Hardware also implicates design patents, which protect ornamental design of functional items for fourteen years.[42] If a developer obtains a design patent, they can bring infringement suits against similar-looking products. The design patent protects "the design embodied in or applied to an article of manufacture (or portion thereof) and not the article itself."[43]

Some open hardware developers might seek to obtain patents on the hardware they develop. However, as with most software licenses, it is then important that an open hardware license contains a patent grant or covenant not to sue licensees, at least to the extent the patent is necessary to implement the provided design. There has been some controversy over open source licenses that attempt to exclude patent grants from the licensor,[44] and licenses that are silent on patent grants are generally assumed to contain implicit licenses.[45] The effect of the patent grant in a copyright license is that someone who fails to follow the terms of the license would not receive protection of the patent grant, and thus would be infringing rights of the licensor under patent as well as copyright, to the extent they are infringing on the licensor's exclusive rights.

The Defensive Patent License[46]

---

42. 35 U.S.C. § 173 (2013).

43. U.S. Patent & Trademark Office, Manual of Patent Examining Procedure § 1502, available at http://www.uspto.gov/web/offices/pac/mpep/s1502.html.

44. See, e.g. Glyn Moody, Should an Open Source Licence Ever Be Patent-Agnostic?, Linux Journal (Apr. 9, 2009), http://www.linuxjournal.com/content/should-open-source-licence-ever-be-patent-agnostic (discussing a license proposal by the MPEG Working Group that explicitly excludes a patent grant).

45. The BSD License is silent on patents, but many open source software users assume that BSD contains an implicit grant. However, this theory has not been tested in court. See, e.g. Bruce Perens, BSD has implicit patent grant, LWN.net (May 25, 2010), http://lwn.net/Articles/388996/ (claiming that "[i]f you publish something under a license granting the right to use and then sue the folks who use it, expect that the judge will not cooperate - you either gave those folks and implicit use grant for your patent or you entrapped them.")

46. www.defensivepatentlicense.com; http://jolt.law.harvard.edu/articles/pdf/v26/26HarvJLTech1.pdf.

The Defensive Patent License (DPL) is a standardized open patent license designed to encourage the creation of a broad, decentralized network of Open Innovation Communities (OICs) that both patent their innovations with a commitment to defensive purposes and license them on a royalty-free basis to any others who will do the same. In doing so, the goal is to build up a collective network of patents that has the same deterrent power as a large proprietary defensive "portfolio" — but a portfolio that has its costs and benefits distributed across the users of the DPL, and that does not require separate centralized management. As such, it harnesses the network effects of OIC distributed cost and benefit structures, the commitment to OIC values, and the reliability of other standard distributed OIC licenses, such as the GPL or Creative Commons' copyleft licenses, and apply them in the patent context.

The DPL operates by creating a set of viral, bilateral obligations focused on preventing offensive patent litigation and promoting freedom to operate and innovate. Specifically, the DPL provides every DPL user a perpetual, worldwide, royalty-free license to every other DPL user's entire current and future patent portfolio, subject to the following four conditions:

i. Every DPL user (licensor or licensee) will forgo any offensive patent infringement actions against any other DPL user;
ii. Subject to Condition 4, every DPL user will offer her entire current and future patent portfolio under the DPL;
iii. Every DPL user will bind any successor-in-interest to any part of her patent portfolio to her obligations under the DPL;
iv. If a DPL user wishes to stop offering her patents under the DPL, she may do so, but only with six months' notice to existing DPL users and future parties. She must continue to

grant, and may not revoke, any licenses that are in place before the end of the notice period. Once she stops offering the DPL, other DPL users are free to convert their licenses to Fair, Reasonable, And Non-Discriminatory (FRAND) licenses at will, but the DPLs she granted previously remain in effect.

All DPLs are irrevocable for the full term of the relevant patents, except if one or more of the above conditions are not met. Thus, if a licensee files an offensive patent infringement action against any other DPL user, then any other DPL user may then revoke the offender's DPL to his patents at any time and, at his option, pursue royalties or enforcement actions against her. Importantly, these obligations and conditions apply only with regard to any others who use the DPL. Any DPL user may independently pursue royalties or enforcement actions against any non-DPL user at any time.

To create administrative transparency and enhance enforceability, the DPL Foundation envisions that certain information about the network of DPL users would be available via a centralized website with a backend tracking database. All DPL users—along with publicly available information about their patent portfolios—would be listed on the site, along with contact information for where to request a license, and a mailing list for new information regarding patents under the DPL.

Thus, the mechanics of joining the DPL network would proceed as follows:

i. An inventor decides to begin offering her patents under the DPL;

ii. She makes this publicly known (via her own website) and registers with the DPL tracking website;

iii. Once registered, the website provides the inventor with a blanket DPL licensing form that she agrees will bind her in relation to anyone who accepts the license;

iv. She then receives access to the pages for every other DPL user with an option to accept any or all of the DPLs for their portfolios. One can also imagine an option to accept all known DPLs in a single click. The website then distributes an acknowledgment of all license offers and acceptances to the participating parties and records them in its internal database. The licenses take effect immediately.

v. As new patents issue or new applications are published for each registered DPL user, they are added to the website, either automatically or by the DPL user herself. Each DPL user may then take additional licenses to newly issued patents either manually or automatically via the DPL website.

vi. If the DPL user chooses to stop offering her patents under the DPL, she registers her six-month Discontinuation Notice at the website, which alerts all DPL users. Six months later, the DPL user's page is updated appropriately but all information related to the user and her portfolio remain preserved. Other DPL users are then given the option to convert any licenses for the leaving user to FRAND as of the Departure Date.

iv. Trademark Licenses

Certification marks

Trademark law can be used to protect open hardware in two different ways. First, it can denote the integrity of an open hardware project through the creation of a certification mark, to the extent the community recognizes such mark as valid and as a sign of assurance. This is important in sensor development because a certification mark can show compliance with a

measurement standard and a commitment to data integrity. Second, a trademark can be used to restrict downstream uses of a design in the sense that non-conforming uses would not be able to claim affiliation to the upstream project.

Several trademark-based models have been proposed for open hardware. Most prominently, the Open Source Hardware and Design Alliance ("OHANDA") has attempted to create a certification mark that can be used on physical hardware that follows their open hardware definition.[47] In software, the Open Source Initiative ("OSI") uses its trademark to certify licenses that it believes are suitably adherent to open source principles (the "open" designation thus trickles down to licensed projects). Certification marks like the OHANDA mark are clearly protected by law; the Lanham Act provides for the registration of certification marks, which are entitled to the same protection as trademarks.[48] While such a mark can denote compliance with community norms and agreed-upon principles, it provides no protection against infringing users who do not copy the mark. Still, the use of "open" trademarks can reduce search

47. OHANDA requires adherence to four principles: "Freedom 0: The freedom to use the device for any purpose. Freedom 1: The freedom to study how the device works and change it to make it to do what you wish. Access to the complete design is precondition to this; Freedom 2: Redistribute the device and/or design (remanufacture); Freedom 3: The freedom to improve the device and/or design, and release your improvements (and modified versions in general) to the public, so that the whole community benefits. Access to the complete design is precondition to this." Open Source Hardware and Design Alliance, http://www.ohanda.org/ (last visited May 1, 2014).

48. 15 U.S.C. § 1054 (1999).

costs when a consumer is attempting to determine whether a project that claims to be "open" is actually so.[49] [50]

Hardware projects have successfully wielded trademark law to exert control over projects and communities. Arduino, a successful open hardware project that provides a prototyping platform for electronics development, has developed and enforced its trademark. While the creators encourage the creation of Arduino-compatible devices, derived from their specifications, they strictly prescribe appropriate use of their mark.[51] In one incident, an employee of Arduino's manufacturing partner attempted to sell a derivative of the Arduino board on Kickstarter, and named the product *smARtDUINO*.[52] Arduino asked for a name change but did not pursue litigation; still, the matter raised serious concern about the appropriateness of using trademarks to protect community-driven open hardware projects.[53] Trademark has also been important to the Linux project, which licenses its trademark rights through the Linux Mark Institute. In order to prevent abandonment of trademark, the Institute requires adherence to its brand guidelines, even

---

49. The Open Source Initiative, which certifies licenses and provides a certification mark, has been successful in implementing a similar program that approves various licenses. The Licence Review Process, Open Source Initiative, http://opensource.org/approval (last visited May 1, 2014) (describing the approval process for OSI-certified licenses).

50. The misuse of the term open is referred to as "openwashing". See, e.g. Klint Finley, How to Spot Openwashing, ReadWriteWeb (Feb. 3, 2011), http://readwrite.com/2011/02/03/how_to_spot_openwashing.

51. See Trademark, Arduino, http://arduino.cc/en/Trademark/HomePage?from=Main.Trademark (last visited May 1, 2014).

52. smARtDUINO: Open System by former ARDUINO's manufacturer, Kickstarter https://www.kickstarter.com/projects/fairduino/smartduino-open-system-by-former-arduinos-manufact (last visited May 1, 2014)

53. See Massimo Banzi, Kickstarter, Trademarks and Lies, Arduino Blog (Nov. 16, 2012), http://blog.arduino.cc/2012/11/26/kickstarter-trademarks-and-lies/ (describing the Arduino trademark controversy).

though use is now free.[54] Open source projects that do not exert sufficient control over their brands might be susceptible to an abandonment claim.

The use of trademark preserves a level of control for the developers of open source software. While many software projects are governed by a democratic mechanism, dissenting programmers can start their own version by "forking" the code into a new project. However, a forked project must take on a new name and thus loses the benefits of the trademark.[55] In open hardware development, engineers would still be able to "fork" a project but would have to remain compliant with the upstream license.

Trademark can also be a useful monetization tool, and can also support a dual licensing strategy where a developer sells its own products under a promoted brand, while allowing others to create the same hardware under a different brand name. Some prominent members of the open source software community have suggested that trademarks have been exceptionally valuable for commercial entities that control open source projects, and have driven up the value of these entities in transactions.[56]

(x) Open Hardware Movement Can Enforce Norms Around Hardware Collaboration

Copyright is useful as a mechanism for software license enforcement, because exact copying can be straightforward to prove, and damages can be substantial. Still, the more important function of open source licensing is to shape and enforce norms for a growing

---

54. Sublicense Agreement, Linux Foundation, http://www.linuxfoundation.org/programs/legal/trademark/sublicense-agreement (last visited May 1, 2014).

55. For an analysis of forking and its effect on software communities, see Linus Nyman & Juho Lindman, Code Forking, Governance, and Sustainability in Open Source Software, Tech. Innovation Mgmt. Rev. (Jan. 2013), available at http://timreview.ca/article/644.

56. Ian Skerrett, Successful trademarks are more important than OS Licenses, http://ianskerrett.wordpress.com, http://ianskerrett.wordpress.com/2008/03/03/successful-trademarks-are-more-important-than-os-licenses/ (last visited May 1, 2014).

community of open hardware developers. Javier Serrano, who works at the European Organization for Nuclear Research ("CERN") and helped create the CERN OHL, said that enforceability is secondary to norm-generation:

> There is some discussion in legal lists as to how enforceable it is, but if people take it seriously, and many do, it can result in a lot of interesting designs being published.[57]

As an example, he cites several projects completed by CERN that were modified, which then felt obligated to license their work under CERN despite the fact that its legal status is uncertain. Similarly, OSHWA's best practices suggest that "[w]hile licensing is a complex subject, use of licenses is an important way of signaling [sic] how others can and should use your work."[58]

This view suggests that open source licenses serve as internal laws, governing the community, more than they serve as external laws. As one open hardware developer said in response to an online discussion about licensing, "An open source project is an institution. It requires some laws [governing] how people interact. Institutions are good for creating value from which nobody is excluded, like open source products… Without the license people are less likely to invest their time or resources in a project."[59] Internal law might be a more useful framework

---

57. Javier Serrano, Re: The Solderpad Hardware License, OH Updates (Mar. 28 2012, 9:26 AM, http://lists.openhardwaresummit.org/pipermail/updates-openhardwaresummit.org/2012-March/000803.html.

58. Best Practices for Open-Source Hardware, Open Source Hardware Association, http://www.oshwa.org/sharing-best-practices/ (last visited May 1, 2014).

59. Andrew Katz, Fwd: the solderpad hardware license, OH Updates (Mar. 28 2012, 1:38 PM), http://lists.openhardwaresummit.org/pipermail/updates-openhardwaresummit.org/2012-March/000806.html.

because of the territorial difficulties associated with open innovation communities, which are often geographically dispersed. This causes significant practical problems related to enforcement in foreign countries, as well as substantive problems related to differing interpretations and requirements under legal regimes. The use of internal law serves as a transnational law that is enforceable by the international open innovation community, rather than the courts of a particular jurisdiction.[60]

In the more mature field of open source software, enforcement actions have been infrequent; although there are currently more than one million open source projects,[61] there have only been a handful of enforcement actions and one court decision in the United States upholding the validity of an open source license.[62] There is also a concern with over-enforcement in the community, namely that visible examples of enforcement will deter even well-meaning corporations from using and contributing to open source projects. After a contributor to the BusyBox project started an enforcement program with the Software Freedom Law Center, use of BusyBox declined and some contributors attempted to create a competing version under a less

---

60. Indeed, the "courts" are the forums, blogs, and listservs that make serve as communications channels for open source contributors. The Software Freedom Law Center, in particular, attempts to enforce community norms through judicial and extrajudicial means. See, e.g. Heather J. Meeker, Open Source and the Age of Enforcement, 4 Hastings Sci. & Tech. L.J. 267 (2012) (describing the legal enforcers of the open source regime in the United States, including the Software Freedom Law Center).

61. Eighth Annual Future of Open Source Survey Finds OSS Powering New Technologies, Reaching New People, and Creating New Economics, Black Duck Software Resource Center (Apr. 3, 2014), http://www.blackducksoftware.com/news/releases/2014-future-open-source-survey-results-revealed (claiming that a commercial open source database has more than one million projects).

62. For a survey of the attempts at litigation over open source software, see Meeker, supra note 50.

restrictive license.[63] This lack of enforcement actions, and the community response to efforts to enforce, demonstrates that the primary value of open licensing is in norm-shaping, rather than actual enforcement of intellectual property rights.

(xi) Standards Organizations & Certification Organizations in Technology Today

Although 802.11 and WiFi are often used interchangeably, they refer to very different aspects of the technologies used to produce wireless local area networks today. 802.11 is a family of standards that was first defined by the IEEE in 1997, whereas WiFi is a trademarked name owned by the WiFi Alliance and reserved for use only in products that have been certified to perform in accordance with its specification for meeting the 802.11 standard. One is a widely adopted practice defined by a community, the other is a trademarked symbol of quality managed by a trade association. The advantage of the WiFi brand is that it ensures a consistent level of quality and interoperability.

In this context, the IEEE promoted the essential intellectual property that provided a new way of extending ethernet networking through the unregulated ISM radio band. This, however, was not a guarantee that following the standard was enough to ensure interoperability of devices from different manufacturers. Accomplishing that goal required not just consensus, but a way to verify the performance of all 802.11 devices, essentially a system of accountability to consumers enforced by a trade association. Without this cooperation, there could little trust between

---

63. Busybox replacement project, eLinux.org, http://www.elinux.org/Busybox_replacement_project (last visited May 1, 2014) (Expressing concern that "[l]itigants have sometimes requested remedies outside the scope of busybox itself, such as review authority over unrelated products, or right of refusal over non-busybox modules. This causes concern among chip vendors and suppliers."); http://landley.net/toybox/about.html; see also Edward J. Naughton, Is BusyBox Too Dangerous To Use?, Brown Rudnick Emerging Tech. Blog, http://brownrudnick.com/blog/emerging-technologies/is-busybox-too-dangerous-to-use/.

manufacturers that standards would be followed, and without that trust there would be little to inspire confidence in consumers.

This model of isolating standards and certifications to promote wider adoption of new technologies is extremely common in the computer and networking hardware industry, but it is not limited to this area. Take for instance, the need for scientific instrumentation capable of collecting data that meets government standards. In the case of water, it would not be possible to enforce the United States' Clean Water Act if there were no mechanism for generating consensus around measurement standards, as well as a mechanism for assessing the performance of different implementations of the standards. As a result, the EPA publishes standards for Clean Water Act Analytical Methods and offers a certification program to guarantee scientists and consumers that products perform properly.

(xii) Different Industries, Different Sensors

Sensors are not, by default, subject to any regulations that do not already apply to consumer electronics.[64] Yet if the sensor is being used in a scientific application or a safety application there are many different rules that can apply.

Depending on the claims a vendor wishes to make about a product there are several distinct categories to consider:

- Medical devices (subject to FDA approval)
- Safety devices (subject to application specific tests or certifications)
- Scientific instruments (may be subject to EPA, USGS or application specific tests or certifications)

64. FCC Compliance Part 15, for example, is mandatory.

- Measurement devices (may be subject to NIST or application specific tests or certifications)

Beyond this, different types of intended end-users result in different regulatory hurdles in each category:

- Highly skilled end-users (i.e. Doctors and Scientists)
- Skilled end-users (i.e. Technicians that have undergone application specific training)
- Unskilled end-users (i.e. anyone who lacks training)

Depending on what combination of end-user and intended application, marketing a given sensor or instrument might present considerable challenges. Generic measurement devices, like personal activity monitors, are easy to market to unskilled users, provided they contain disclaimers asserting they are making no scientific or medical claims. However, should a new class of FDA approved health monitors come to market (as is speculated with smart watches), they would offer a great deal more credibility, not just to end-users, but to third-parties, such as doctors and insurance companies, which would open new doors for the use of data in healthcare. Marketing a "smoke alarm" requires UL 217 certification (UL 2034 is required for carbon monoxide as well), but an "air monitor" making no such claim requires no approval. There are many such "air monitors" available today in kit form, but there do not exist any legal mechanisms to verify the integrity of data collected by such a kit, since certification, in its present form, tests the performance of finished products.

What is important to recognize in these dynamics is that well-tested and well-engineered devices have the potential to put medical-grade data in the hands of ordinary people without the need to rely upon experts. Getting there, however requires meeting two very complex

challenges: generating consensus around a measurement standard, and certifying that a given sensor or device performs in accordance with the standard.

(xiii) Preliminary Conclusions

Purely "open" hardware, as designated in today's prevailing licenses, generally forbids any restrictions on use. As has been suggested by Phil Torone and others, this is generally seen as a strength for the Open Hardware community, and is responsible for large-scale collaborations that have helped to standardize many aspects of hardware development, promoting efficiency, reliability, diversity, while lowering the barrier of entry for new hardware developers. Each of these characteristics is vitally needed in the world of sensor development, however they need to be translated to address the unique needs of sensor technologies.

Establishing trust in large-scale decentralized data collection efforts requires careful coordination at all aspects of sensor design, integration, implementation and data analysis to ensure consistently accurate data, and to enable legally sound and scientifically verifiable claims using such data. This will require standardization of specifications, testing and evaluation protocols, and 3rd party organizations capable of certifying the performance of different sensing methods.

Today there are already some certification processes in existence. Beyond FDA certification in medicine and legally required certifications for safety devices, there are other examples in science that are establishing the kinds of standardized practices and testing protocols that sensors require. For example, in the world of seismometers, USGS has detailed 60+ page

guidelines including ranges to use when certifying seismometers.[65] Even when the seismometers are returned from the field, the IRIS PASSCAL[66] Instrument Center tests them to ensure they are working within the established ranges much like an aircraft goes through checks after each flight or a car goes through checks every 10000 miles. Established consumer devices are typically certified by standards and certification bodies such as ISO or NIST. Alliance for Coastal Technologies (ACT) conducts Technology Evaluations including Verifications and Demonstrations. Technology Verifications focus on classes of commercially available instruments to provide confirmation that each technology meets the manufacturer's performance specifications or claims and/or provides verified data on those operational parameters that stakeholders require to make a use decision. Verifications are a 25-step process, which includes community consensus on test protocols, laboratory and field-testing, and QA/QC based on EPA and ISO guidelines. Field tests are carried out at no fewer than four but typically all six ACT partner sites.

Although certification can be carried out by the government or established 3rd party certifiers, there is no reason why open development communities cannot build their own structures to accomplish this as well. The essential ingredients of such frameworks are:

- A community with a vested interested in a given sensing method
- Agreed upon standards for measurement, specifications, performance metrics, and assessment protocols

65. Charles R. Hutt, John R. Evans, Fred Followill, Robert L. Nigbor, and Erhard Wielandt. 2009. Guidelines for Standardized Testing of Broadband Seismometers and Accelerometers. USGS. http://pubs.usgs.gov/of/2009/1295/.

66. Program for Array Seismic Studies for the Continental Lithosphere (PASSCAL)

- Agreed upon certification procedures for supporting data integrity claims
- An organization run by the community that manages permissive licensing of copyrighted and patented intellectual property and leverages trademark to signal which sensors and devices have passed its certifications

There are many possible implementations of this formula, and different markets and sensing paradigms will require different approaches to it. Possibilities may include:

- A centralized organization that manages both performance certification, and Defensive Patent Licensing of the standards essential IP necessary for a given sensing technology
- A decentralized network of certification labs that coordinate and collaborate with open development communities to endorse certification methods
- Widespread commercialization of calibration standards and devices that simplify the process of end-user verification and maintenance of devices.
- Private companies opening up their own sensing hardware to promote it as a standard using mechanisms like DPL and trademark to perform certification of 3rd party devices themselves.

What will be essential to any implementation is the development of an organizational structure that maximizes quality and trust most efficiently. These structures will not solve all problems with sensors or address the cultural implications of distributed sensing and the increasingly autonomous machines that sensors enable, but they have great potential to support the coordination and consensus building that will be required in any future where sensors widely proliferate. One issue that will need to be addressed will be the proprietary status of data collected by sensing hardware, and whether it is ethical or legal to build restrictions on data into

sensing hardware and devices. This will present major dilemmas for companies, developers, legislators, and civil liberties advocates. What is clear is that no thoughtful conversation about such issues will be possible without a deeper technical understanding of how such technologies work, and embracing the structures outlined above or better alternatives may provide a stable foundation when that time comes.

APPENDIX

I. Calibration discussion

The following email thread is about calibration of sensors is from the sensor-in-journalism mailing list.

Javaun Moradi <j…com>: “The challenge of air is a lot harder than many of the other sensor areas. Pollutants interfere with each other, some canceling each other out, some boosting the readings of others. Inexpensive metal oxide sensors also are affected by temp and humidity, which is why we added those sensors in Chicago and attempted rough calibration in the software layer.”

Kevin Webster <k…com>: “To Javaun's point, a lot of the inexpensive oxidizing and reducing gas sensors out there, including the one in the Sensordrone, are good at "weighing total volume", but bad at telling you what's in that volume. The analogy we often use is this: I have ten pounds of fruit. Some apples, some oranges. I can tell you (most of the time) that there's 10 pounds there, but it's harder to tell how much is apples, and how much is oranges. The rough calibration he speaks of (not to include you in the third person, Javaun, my apologies) is based on estimates of how much, in normal circumstances, would be apples, and how much would be oranges. But it's not true every day. And some days, someone adds a banana. Our patented sensor is really really good at carbon monoxide, and H2S. But the other gas sensor in the Sensordrone is more ambiguous. It needs context that a catch all type device can't provide.”

Don Blair <d…org>: “This is an issue near and dear to my heart. Thanks, everyone, for your thoughtful contributions. Kevin -- love the 'pile of mixed fruit' analogy. A similar analogy we've been employing in the context of water quality monitoring, where the conductivity of a water sample is a key parameter, is that measuring the conductivity of water is akin to measuring body temperature in human health: a thermometer can tell you that you have a fever, and indicate that something is unusual; but a fever doesn't point to a particular causal agent or disease. For a specific diagnosis, you'll need a lot of other contextual information, and likely further, more extensive (expensive) tests. One imagines that there are many useful applications even for 'low veracity' sensors. By aggregating a lot of data from such systems, and combining it with other auxiliary information, it will in many cases be possible to come to develop useful models / make good predictions. For example: one could imagine that even if the GPS tracking ability of smart phones were rather poor and low-resolution, the aggregated statistics of e.g. commuters during rush hour would tend to produce quite accurate predictions of traffic flow rates by averaging out all of the noise. Similarly, low-veracity environmental monitors could, with sufficient statistics, be used to generate quite reliable "hot spot identification" maps that would allow e.g. the EPA to deploy higher-cost, more intensive monitoring equipment only where it was most needed. The trick in all this, I suppose, is to be as clear and as conservative as possible about the sensitivity and accuracy of one's instrumentation. This is made difficult by a consumer-driven, Kickstarter

'gadget' culture that is looking for an iPhone-like, point-and-click, app-like simplicity in everything, including environmental monitoring. It's simply the case that for many environmental concerns -- water quality, for example -- we're very far away from having a device that can be dipped in the water and spit back "good water!" or "bad water", as per the Star Trek fantasy. Hydrologists won't be out of a job any time soon."

Kevin Webster <k…com>: "Great points, Don. In some ways, I think that when we won the NASA Tech Briefs Award it accidentally lent a layer of credibility to the whole class of devices, of which we were one of a handful. It became very difficult to "sell down" from there, despite us telling people "Look, you're not replacing a $2000 scientific analyzer with this.". The problem is, people wanted to. And they were going to try. While we never ended up in an article like the one that started this discussion, I empathize with AQE. I have a lot of respect for their work, and these days it almost seems harder to convince people of what your device CAN'T do rather than what it can. Buyers are letting their wishes and their imaginations almost develop a feature set, in this case, absolute accuracy, that isn't published in the docs, nor even included in the marketing message. I think a better use of devices like ours, until such time as we nail down purpose driven variations, is to monitor for change, and not to monitor for precision measurements. There's a myriad uses for that kind of data, and it's actionable. However, if you need to get to the molecular level, you're still going to need to walk down the hall and ask for a larger budget."

Peter Sand of Modular Science and Manylabs: "The sensor manufacturers provide data sheets for that specify the behavior and ideally variance between individual sensors of a particular type. If the sensor is sufficiently expensive it may be individually calibrated at the factory (and arrive with the the calibration info). For cheaper sensors you can either live with the variance or do your own calibration."

II. FDA regulatory path for medical devices:[67]

	Description	Class 1 Devices	Class 2 Devices	Class 3 Devices
510 (k) exempt devices	Clinical chemistry and clinical toxicology devices Hematology and pathology devices Immunology and microbiology devices Anesthesiology devices Cardiovascular devices Dental devices Ear, nose, and throat devices Gastroenterology-urology devices General and plastic surgery devices General hospital and personal use devices Neurological devices Obstetrical and gynecological devices Ophthalmic devices Orthopedic devices Physical medicine devices Radiology devices	X	X	
Premarket Notification 510 (k) devices	To prove substantial equivalence to an existing device	X	X	X
Premarket Approval (PMA) devices	Inidividual license for marketing a new device, or for a device designed to support or sustain human life			X
Humanitarian use devices (HUD): Humanitarian Device Exemption (HDE)	For treating conditions that affect less than 4000 people/year in the US. Similar to PMA, without the requirement of proving the effectiveness of the device			X

67. Ham, Scott, “Mapping the Medical Device Development Process”