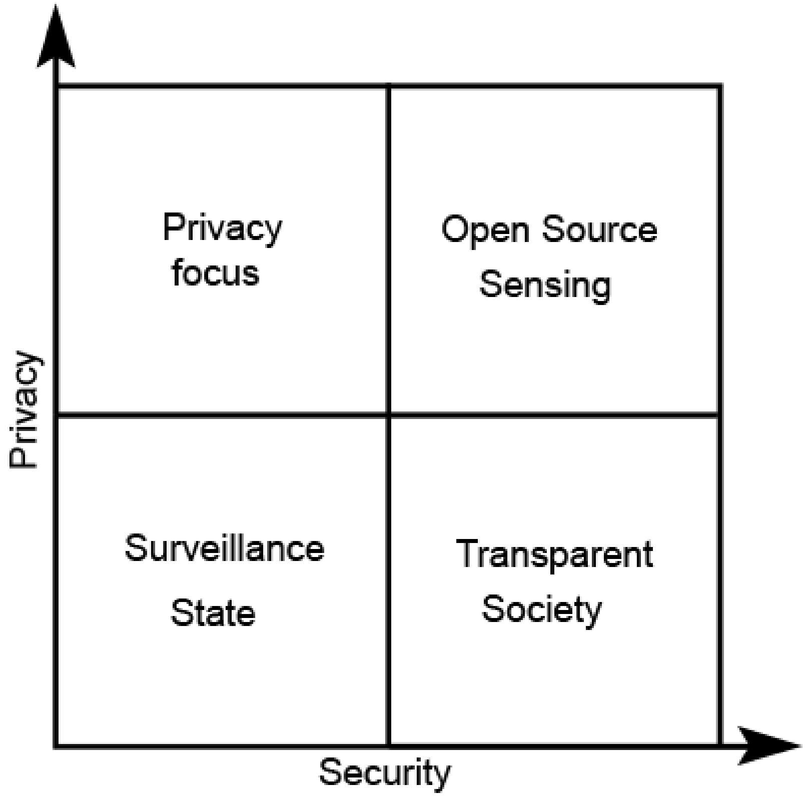

Citizen-Controlled Sensing:
Using open source & nanotechnology to reduce surveillance
& head off Iraq-style wars

Version 0.6

DRAFT -- COMMENTS REQUESTED

Christine Peterson
Foresight Institute
May 2009

Summary

Since 9/11, the U.S. and some other governments have increased their Surveillance State behavior, both internally and externally. Yet this surveillance still often fails: faulty intelligence data on suspected weapons of mass destruction helped lead to the current costly war in Iraq.

As global GDP per capita increases and the costs of weapons of mass destruction (WMD) decrease, both realistic and unrealistic fears will increase, encouraging ever-more surveillance by governments — unless another approach to the issue can be found. The space-based monitoring

that has served us relatively well for nuclear weapons will be far less effective in checking for biotech and, eventually, nanotech-based weapons.

We have a choice: accept the top-down Surveillance State pathway the U.S. is now following, or develop a “bottom-up”, decentralized, open source approach to WMD sensing and defense. This proposal sketches some steps toward the latter: citizen-controlled, privacy-oriented, verifiably-limited open source security devices and procedures focused on obtaining and sharing the *minimal* data required for communities to satisfy the reasonable concerns of their neighbors — international and domestic — regarding the possible presence of specific weapons able to affect those neighbors directly.

The goal is to use decentralized, open source approaches to address legitimate security concerns without impacting personal privacy in other areas. In the long term, open source defensive technologies will likely be the only ones capable of keeping up with rapidly-advancing offensive technologies — just as open source software is faster at addressing computer viruses today.

Like other open source projects, this proposal would not involve government approval or participation, though it is hoped that the data produced will be accurate enough to be used by governments for arms control monitoring purposes.

The problem

As technology advances, individuals and small groups are empowered. The vast majority of their applications of new technologies are meant to improve the human condition, but a few are not. Over time it is becoming technically easier to misuse radiological, chemical, biological, and eventually nanotechnological materials and devices.

Since 9/11, concern about heading off terrorist attacks has led to increasing efforts by governments to conduct electronic, video, and chemical surveillance of citizens, including over-reactions which arguably violate civil liberties. To date, many citizens are tolerating this change, being under the impression that it is necessary if we are avoid great loss of life to future attacks. Only a few organizations, such as the Electronic Frontier Foundation, have stepped forward to try to head off this new surveillance via a series of lawsuits.

This ongoing conflict between governments' desire for increasing surveillance and individuals' desire for privacy will continue, but as time passes and violent incidents become easier to carry out, society will feel pushed toward either the Surveillance State or Transparent Society models. In these models, a wide variety of surveillance data is collected and either kept under the control of government (Surveillance State) or widely distributed to the public (Transparent Society). The Transparent Society model was developed in response to a belief that increasing surveillance is inevitable and that governments would misuse data; advocates of this model hope to limit that misuse by distributing collected information widely to the broader society.

The best-known proponent of the Transparent Society is David Brin, author of a book of the same name (ref 1). The best-known critic is Bruce Schneier, a leading computer security expert who responded with "The Myth of the Transparent Society" (ref 2). This debate has continued in *Wired* magazine and at the Computers, Freedom & Privacy Conference (ref 3,4).

In parallel with this intellectual conflict, numerous new surveillance projects are being carried out. As this is written, no significant terrorist incidents have occurred in the U.S. since 2001, but we can expect that when the next incident occurs, these sensing and recording devices will be promoted as part of the solution. Fear — both real and manufactured — will continue to push society toward a Surveillance State model. The current proposal attempts to redirect these concerns into practical, decentralized, voluntary action to address the actual problem while maximizing privacy.

A possible third pathway

There is a community of thought available that may provide a third model, giving us an option separate from both the Surveillance State and Transparent Society. The software community, and specifically the open source community, routinely grapple with tradeoffs between security and privacy while simultaneously attempting to maximize both functionality and freedom. Compared to most national security professionals, their understanding of the key issues is strong. These values and technical skills could be applied to security in the physical world as they already are in the software world.

Open source approaches have already spread well beyond software development; the "open source hardware" concept is gaining support (ref 5). Another term beginning to be used is "community electronics".

Here it is proposed that this approach be applied to the question of security from terrorism. Specifically, rather than develop closed-source, proprietary sensing and recording devices, we could instead design, build, and operate devices based on open source hardware and software which can verifiably detect only actual materials of concern, rather than tracking the location and behavior of individuals and the presence of non-weapons materials (e.g., illegal drugs).

A thought experiment is of use in exploring this idea. Two materials which have been used in well-known attacks are anthrax (NYC; Washington, DC; and Florida in 2001) and sarin (Tokyo subway in 1995). Ricin, a highly toxic substance, has also been produced for use in terrorism (ref 6).

It is reasonable for individuals and communities to require knowledge of the location of these three materials when they are near enough to cause a potential security problem. An open source project to build a sensor able to detect one or more of these materials, and verifiably able to detect nothing else, might be an appropriate demonstration of the approach. Such a project would need to include attention to software, manufacturing, and data distribution as well as detection of the substance. In every area, it would be critical to be able to verify that the process actually implemented matches the open-source design.

Communities — of varying sizes, from multi-country regions to households — could specify the physical locations they regard as relevant to their own security, which could vary by specific material. Requesting such information would imply the reciprocal willingness to supply similar information from one's own location, i.e., if our community requires anthrax location data within 500 km, we are willing to permit export of anthrax data about our own location to those within the same distance from our border. Negotiating and implementing such data exchanges would be a complex task; well-designed software would be key to success.

Participation in the project could be on the same basis as other open source projects. Government employees and even military employees might participate as they do in many open source efforts, agreeing to follow the usual community standards.

A pilot project focusing on one or a small number of substances could be expanded to detect and track other materials of concern, e.g., cesium-137 and americium, which are used in commerce but also of potential use in "dirty bombs".

If successful, such open source monitoring devices could be used by countries wishing to reassure other countries having arms control concerns, thus eliminating the perceived need for involuntary entry by armed forces to carry out forcible inspections.

Educational role of the project

In addition to the practical value of the device or devices that might be built, discussion of the project would introduce and advance the concept that citizens should insist on open source hardware and software in sensing devices made for public security purposes, including verifiability regarding which substances are being detected.

In the long term, as defense technology becomes increasingly automated, we can expect detection of problem substances to trigger actual physical action in response. We can introduce the concept that such action should also be performed based on open source principles.

Spreading the concept of the desirability of having critical public systems built on open source hardware/software/data-handling principles should also be of use when attempting to set public expectations on issues such as electronic voting.

Anticipated challenges

We can expect that some security professionals in government will not appreciate a civilian effort in open source sensing. An indication of this is the recent "proposed law in New York City that will require people to get a license before they can buy chemical, biological, or radiological attack detectors". (ref 7)

Leadership role of technical community

In an *LA Times* editorial, Tim Rutten wrote of the revolt of JPL staff against excessive security inquisitions into their private lives. Rutten asked, "Who would have guessed that the folks with the pocket protectors would turn out to be the ones with the right stuff?" The technical community, and the open source software/hardware community in particular, have an opportunity to change how society thinks about security — away from fear-based surveillance and toward trust-building voluntary collaboration.

Initial project steps & budget

This is an extremely ambitious project which will take decades to implement fully and require major changes in how citizens think about security. Yet the proposed perspective fits well with traditional understandings of American collaboration and bottom-up-style government.

The first step will be to flesh out and refine the concepts among the most relevant communities. As a start we propose a one-year project with these stages: initial workshop, interviews with key thought leaders, collaborative editing of draft documents via wiki, production of a policy white paper, and a concluding workshop to plan next steps.

The budget for this one-year project could range from $50K to $150K, depending on travel costs and the ratio of volunteer to staff support.

This project is in the earliest planning stages. Your comments at this time can help the effort get on the right track at its start. Financial support is needed to move this forward; donations are tax-deductible in the U.S. as charitable donations.

Organizational contact

Foresight is recruiting organizational partners as well as individuals who wish to explore these ideas. Foresight is currently serving as organizational contact and fundraising lead. For more information please contact Christine Peterson, Vice President, Foresight Institute, peterson@foresight.org, tel +1 650 289 0860 ext 255.

References

Ref 1: http://www.davidbrin.com/tschp1.html
Ref 2:
http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0306
Ref 3: http://www.wired.com/politics/security/news/2008/03/brin_rebuttal
Ref 4: http://en.wikipedia.org/wiki/The_Transparent_Society
Ref 5: http://en.wikipedia.org/wiki/Open_source_hardware
Ref 6: http://en.wikipedia.org/wiki/Ricin
Ref 7: http://www.schneier.com/blog/archives/2008/01/locked_fire_box.html