COMMUNITY POLICING BY THE COMMUNITY

A Model for Community Policing
By the Community
Powered by Community Broadband

June 2010

David Billstrom
Craig McClure
John Teeter

of OpenCommons.org

SUMMARY

Leveraging the wisdom of crowds, a culture of social networking, ubiquitous cell phones and modular software gleaned from open source platforms -- the safety and security of a building, a neighborhood, a city can be dramatically improved without significant expense to the municipality or the building owners. Over time costs are actually reduced, benefiting from the power laws inherent in technology (such as Moore's Law) and the increased efficiency of beleaguered law enforcement agencies.

This paper discusses the concepts of a modernized "Neighborhood Watch" system that is hosted in the Cloud, connects neighbors to each other and to public safety services, and can scale from a single building to a large city.

Pilot projects are proposed for several buildings, each in different neighborhoods or EcoDistricts, in Portland, Oregon. Portland is frequently a model for "smarter cities" and consists of approximately 100 neighborhoods of various sizes and constituencies. The concepts tested in the pilot projects should be applicable to any building or neighborhood, in nearly any country, provided sufficient IP bandwidth is provided to the home.

GOOD NEWS / BAD NEWS

The concepts of community policing are well understood and extensively documented elsewhere[1] with general agreement that citizens collaborating in trusted relationships with law enforcement officers leads to less violent crime and increased sense of safety, which indirectly benefits property values.

The bad news is that a variety of difficulties confront communities that contemplate (or already enjoy) community policing – chief among these the lack of institutional memory in the police department regarding a particular neighborhood and an inefficiency among neighbors in communicating with each other about potential threats (and victories). Even where "institutional memory" is preserved, developing the database and keeping it current is an expensive proposition for municipalities facing continued budget contractions.

Police department "memory" about a neighborhood is the product of officers collaborating directly with passionate citizens, which is itself the result of relationship-building by the officers. When the officer is re-assigned (perhaps as a result of their excellent community policing activities) he or she takes the relationships with them to their new assignment, leaving their replacement to re-establish relationships all over again. There is no visible solution to this issue, although some departments have created databases of information[2], these databases are typically focused on criminal elements, rather than collaborative relationships with the community.

Ideally, relationships between collaborative officers and interested citizens would be preserved, or at least referenceble, and even the relationships *between citizens* not just criminal elements, would be visible to police officers.

Citizen-initiated community awareness, such as neighborhood watch groups and "block parent" programs depend upon regular and periodic communication, both to distribute information and also to keep the "network" of participants in the group alive and functioning for emergencies. During a specific threat or incident, the "network" of participants becomes more active and information flows back and forth between the participants.

Several issues challenge the efficiency of these communication networks – first, an increasingly mobile lifestyle means that citizens may move out of the area (or move into the area) and their absence (or sudden arrival) may corrupt the dependability of communications. For example, the "phone tree" is only effective if each node in the tree still lives in the neighborhood. Second, the busy lifestyles and travel schedules, particularly of working professionals, mean that they may be temporarily away from the neighborhood when trouble arises. Third, the group will typically have even less institutional memory than the police department – with no technical or administrative support, the demands of

[1] U.S. Department of Justice. *Community Policing Defined.* Document e030917193
[2] Wilson, Craig, FBI. May, 1997 *FBI Law Enforcement Bulletin: Gang Monikers.*

more-than-full-time jobs and parenting, there is even less opportunity to build a history of events, let alone maintain it for archival search after an incident.

A POTENTIAL SOLUTION

Both the issues of memory within the police department and memory within the neighborhood groups can be addressed by modern technology, essentially by providing a platform and an environment that encourages, facilitates and captures (or "records") the communications between the neighborhood participants. This nails the proverbial two birds with one stone, by enhancing communications within the neighborhood group, and at the same time, building a priceless history of the neighborhood threats and activities for use by police.

A loosely-formatted database of messages – starting with the text in email – can be collected as the neighborhood participants interact about specific threats and events. This data can be kept indefinitely, for use immediately or long after an incident occurs and inspires investigation by police. The flow of information between neighbors has the intangible benefit of also binding their interests together, establishing a style of communication and collaboration, and also provides the tangible benefit of specifically identifying threats and potential threats.

The data itself can even be improved by a continual process of data normalization in which named (and vetted) volunteers from within the neighborhood group (aka "Moderators") can cull the raw data for significant items, edit, and otherwise organize the data so that subsequent search/browse activity of the data reveals more relevant information, more effectively. Essentially, such Moderators are ratified by their neighbors as trusted and skilled "scanners" of information. These already exist in every community; they only need tools to be placed in their hands to facilitate the effort. Done right, the tools should be easy to use and hosted on a variety of platforms (e.g. home PC, smartphone in hand, etc.).

Experienced technologists will recognize the overall concept as conceptually a combination of Facebook –like and Twitter –like social networking tools, with some of the aspects of the crowd-sourced Wikipedia environment. Also relevant is the concept of a “knowledgebase” as utilized by customer service reps and technical support in private industry worldwide – a library of information available for search and browse, which is constantly dynamically expanding as a result of many authors making contributions. 3-1-1 systems also utilize a similar knowledgebase, providing further leverage as the community policing database scale-up to the size of a city.

LONG-TERM VIEW

The inherently cooperative nature of using the tools builds the relationships within the neighborhood, and as such, could further evolve to include more than the text/email messages described above. Additional data types would evolve to be included in the effort:

- Photographs, particularly from smartphones
- Video (ad hoc) from smartphones
- Video from fixed cameras, connected via IP
- Voice conversations on telephones, where participants essentially narrate what they see/witness/observe when typing isn't possible or desirable (and automatically translated into text for archival purposes)
- Voice conversations on radios, where participants use walkie-talkies in their community (should they choose to conduct patrols)
- Push to Talk "walkie-talkie" style direct communication on smartphones
- Geotaggging of event entries

As with the text in the database, these data types can also be further processed from raw into normalized data. For instance, photographs could be "tagged" as people in images on Facebook are tagged by volunteers. For instance, "Joe" who can often be found dumpster diving, is tagged on a photo snapped by a member who observes him in a dumpster. The tagging can also occur after the fact, by a Moderator who for instance may recognize and identify "Joe" when scanning images previously snapped by other volunteers.

ISSUES AND CONCERNS

Privacy. Obviously the participants opt-in to the cooperative effort are explicitly sharing certain aspects of their privacy, and this would be explicit and overt in all materials and tools. Correspondingly, any citizen/resident can opt-out (the default) should they choose, at any time.

On the contrary, we expect most interested citizens to "opt-in" to the project. As trusted relationships among neighbors often carries a very high degree of social intimacy – for instance I ask my neighbors to keep an eye on my house while I am gone on vacation. I am trusting that they will not use the information that I am gone on vacation to steal my belongings while I am gone. In fact, I may give them a key to my house for use while I am gone, either temporarily but perhaps even permanently.

Vigilantism. Over-eager participants could see themselves as a police agency themselves as commissioned to enforce the law. Not only are there numerous examples of how this specific issue has been treated among existing Neighborhood Watch groups across the Nation, but the peer pressure that leads to the sharing of private information will also enforce reasonable limits on participants who tend in this direction. Ultimately, any member can be prohibited from using the tools provided under this concept.

PRELIMINARY REQUIREMENTS & SPECIFICATIONS

Security. Obviously a key requirement for the collaborative environment and database is for security; the information and communication between participants must be held secure from non-participants.

National initiatives for cyber-security are bringing together both requirements and solutions in the areas of privacy, security, and auditing of personal information[3]. This project will follow and support the relevant areas of this national infrastructure.

The system is to maintain graduated security roles as defined in the National Institutes of Standards and Technology (NIST) security framework. These roles are to be mapped to the applicable organizational roles within the various participants of the project.

Community Member Interactive Platforms - The pilot should provide interactive services to the participating communities and community members. The goal is to leverage public access communications facilities and to provide interoperability with private services and carriers through standards based communications facilities.

> **Internet Web Browsers** - Web browsers, such as Firefox, Microsoft Internet Explorer, and Google Chrome provide a basic platform for interaction with the proposed community services.
>
> **Mobile and fixed line Telecommunication Devices** - Telephones and Cell phones are to be used to provide both incoming (demand driven) and outgoing (information notification) communications capabilities. Provisioning of interoperability and
>
> **Radio and Push-To-Talk services** - Integration with public services and first responder communications networks is to be provided for escalation of event responses.

Data Types - Information sourced from community members is to be exchanged, archived, and analyzed by the facilities within the proposed system. Text (SMS) messages and electronic mail (EMail) represent the first and lowest fruit on the tree. Voice via telephone, cellphone and walkie-talkie are to be supported. In addition to these basic Multipurpose Internet Mail Extension[4] (MIME) types, photographs and video clips, as created on cell phones are to be supported.

Information Access - Changes in status, and especially alerts, must be pushed out to subscribers to the system, which will include specific community police officers (at their request and after authorization) as well as to any members of the community.

[3] NIST Computer Security Division Special Publications (800 Series)
[4] http://en.wikipedia.org/wiki/MIME

Scale - The design must anticipate as few as 4-5 contributing members when deployed at the scale of a single building of 15-20 units. The platform upon which the services are deployed must scale appropriately to accommodate a wide variety of community based organizational structures. There is no optimal predicted (or constrained) size of any community and is required that the number of communities supported by unbounded.

Interoperability - The pilot platform must include facilities that allow for information to be passed to external community infrastructure facilities. A common representational format. A public services XML[5] Schema will be defined. Interoperability will be achieved through integration with industry wide standards for information exchange.

PROPOSED PILOT PROJECTS

At least three location/configuration combinations should be piloted with the technology, so that anomolies in any one pilot do not unduly bias the conclusions. Primary consideration for location selection include:

- Existing broadband to (nearly) every resident/participant
- Interest/engagement from at least 10 members of the location
- Within the City of Portland

Using this criteria, the following locations are proposed:

- #1 "Alpha" -- Inner South-East Portland neighborhood (to be determined)
- #2 "Beta" Portland State University EcoDistrict
- #3 OHSU EcoDistricit

A Phased Approach to Service Provisioning:

total: 12 months - with project reviews go/noGo at each phase point.

Phase 1 (2 months) -- Alpha Release to #1 Location

- Provide basic operational prototype of services and facilities to restricted (Alpha) community
- Train and orient participants from #1 Location
- Configure and Document Alpha services platform
- Implement and Document initial mobile application
- Implement and Document initial Web Browser application

[5] http://www.w3.org/XML/

Phase 2 (3 months) -- Beta Release to #1 and #2 Locations

- Provide Beta 1 Level Services Platform to selected community organizers
- Train and orient participants from #1 & #2 Locations (and selected "previews" for #3 Location)
- Configure and Document Beta 1 Services Platform
- Implmement and Document Beta 1 Moble Application(s)
- Implement and Document Beta 1 Web Browser Application(s)
- Provide Alpha Interoperability with Portland Public Services Organizations (Police, Fire, Health)

Phase 3 (7 months) - Full Release to #1, #2 and #3 Locations

- Provide Supported Release of Beta 2 of Services Platform to 3 targeted communities
- Train & orient all potential participants
- Configure and Document Beta 2 of Services Platform
- Implement and Document Beta 2 of Mobile Application(s)
- Implement and Document Beta 2 of Web Browser Application(s)
- Implement and Document Beta 1 Interoperability.

IMPLEMENTATION & EXPANSION

It is vital that the concept and the enabling tools/platform/environment are constructed at minimum cost, maximum performance, and to standards (and emerging standards) with maximal leverage of open source software. Hardware used should similarly be industry-standard (e.g. TCP/IP, …). Proprietary solutions should be avoided.

This is not only a focus to contain cost and speed implementation, but with a view towards compatibility with a large range of open government initiatives, which will likely similarly be constructed using open source software and industry-standard hardware.

The evolution of viable open source, publicly licensed will be key to the success of Government 2.0 as envisioned by the Open Government initiative:

> "Social Media and Web 2.0 define activities that integrate technology, social interaction, and content creation. Social media tools use the "wisdom of crowds" to collaboratively connect online information. Through social media, people or groups can create, organize, edit, comment on, combine, and share content. Social media and Web 2.0 use many technologies and forms, including RSS and other syndicated web feeds, blogs, wikis, photo–sharing, video–sharing, podcasts, social networking, social bookmarking, mashups, widgets, virtual worlds, microblogs, and more."[6]

The Open Commons has been formed to provided a platform to extend these enabling technologies to the community level. The community policing platform discussed in this paper provides services that provide a sense of "We're in this together" that is spacial as well as social. It is about planning and converging public thought into action.

Services and Applications presented to community members through this evolving public platform provide the opportunity to evolve the infrastructure costs of those communities. For example, communities that effectively maintain the livability parameters of their neighborhoods will see reduced need for additional police officers, and could, in fact, lead to a need for fewer officers. An overall savings with a customer base, the community members, that are engaged daily with the maintenance of their community environment.

Over time, the growth of the public infrastructure should encourage innovation in delivery of services of all types. A common, publicly available, technology and communications platform is a shared community resource that can enhance this innovation and be leveraged through a wide variety of innovative applications. Open and shared public access to services through shared media is seen as a key enabler for transforming the nature of our engagements with governmental services providers.[7]

[6] http://www.usa.gov/Topics/Multimedia.shtml
[7] http://en.wikipedia.org/wiki/E-Government

CONCLUSION

Leveraging the wisdom of crowds, a culture of social networking, ubiquitous cell phones and modular software gleaned from open source platforms -- the safety and security of a building, a neighborhood, a city could be drastically improved without significant expense of the municipality or the building owners.

The pilot projects proposed could be implemented for low cost, without a significant impact on existing city staff. The concepts tested in the pilot projects should be applicable to any building or neighborhood, in nearly any country, provided sufficient IP bandwidth is provided to the home.

For More Information:

David Billstrom: davidb@opencommons.org 206-304-8500
Craig McClure: craigm@opencommons.org 503-519-4312
John Teeter: johnt@opencommons.org 208-249-6996

About OpenCommons.org

Open Commons is dedicated to providing a platform for public policy, entrepreneurism, and technology that dramatically improves the communities in which we live -- whether inner city, urban, rural, or undeveloped within the U.S. and throughout the world. We assume that community development will be driven by the desire of people for safety, neighbors and quality of life rather than by technology. We believe there there are many opportunities to enable "market driven" development of community via open source technology, collaboration, and entreprenurial for-profit and non-profit organizations. Just as supply chain optimization has transformed global businesses from building inventory in search of distribution ("push") into on-demand production ("pull"), we want to help individuals pull the value they want into their communities. We want to improve the world we live in.

About the Authors

David Billstrom has experience as a Fortune 100 corporate executive (Intel, Disney) and as a venture capitalist. He also co-founded four companies: Media Mosaic, Quando (now Infoseek/Disney), National Interop, and FBR CoMotion Venture Capital. He has advised, invested in, or served on the board of directors of 17 other companies, across a wide range of industries and markets.

David began as a software engineer, and then software manager, in small companies in the early 1980s where he developed, launched, and supported software products such as point-of-sale systems, early database tools, corporate accounting systems, and compilers on DEC PDP-11 systems and MC68000 UNIX workstations. From 1986 to 1993, he was part of the team at Intel Corporation (INTC) that built and deployed the first commercially available massively parallel supercomputer. He worked in a variety of roles including product management and specification, product launch, marketing, sales, and public relations. David was based both in U.S. and in Europe, with time in Japan.

After departing Intel, he co-founded an award-winning CD-ROM development and publishing firm (Media Mosaic), which was an unsuccessful business, but led to the creation of a specialized Internet search engine in 1996, called Quando. Quando's technology inspired the acquisition of the company by Infoseek (SEEK) and Disney (DIS) in 1999. After the acquisition, he moved to Seattle and served as a vice president at Disney, responsible for content services for the Go internet portal. After Disney, he co-founded a venture capital fund with Friedman Billings Ramsey (FBR) in 2000 and for six years worked with a variety of technology startup companies in Portland, OR, Seattle, WA and in the Silicon Valley.

David is also a member of the board of BrightWorks Northwest (LEED consulting firm for green building development based in Portland, OR with nationwide clients).

David is also a passionate believer in affordable, standards-based, open software technology for public safety agencies. He founded National Interop, Inc. in 2005 to guide public safety users through the adoption of innovative technologies. He serves as chairman of National Interop, and speaks widely on issues of public safety communications. He has testified in state legislatures, local governments, and U.S. Senate hearings on the issues of communications and public safety interoperability.

He is also a first responder with 29 years of experience, with certifications in structural and wildland firefighting, search and rescue, and Department of Homeland Security's COM-L program. He is a former EMT.

Craig McClure as General Manager of National Interop equips first responders throughout the Pacific Northwest with technology to make their jobs more safe, effective while saving lives. His work includes computer dispatch systems, software radio consoles ("Radio Over IP") and tactical communication systems (radio and telephone) that can be deployed at the scene of an emergency by non-technical police officers, firefighters, and EMTs.

Craig is an experienced manager of large-scale ROIP system staging, deployment, monitoring and maintenance having completed several national scale deployments of ROIP systems, which leverage public internet connectivity yielding 98%+ uptime and reliability.

He is a volunteer first responder with 9 years of experience in the Northwest as a Search and Rescue canine handler, ground searcher, and a member of the Mt Hood SAR Council. He has served on the Board of Directors for two non-profit SAR organizations.

He is an instructor of communications and software courses for first responders, and a certified instructor for Lost Person Behavior used in search and rescue.

John Teeter brings a 40 year history in technology industries. Most recently, he has engaged in consultations with Masdar, IBM, and CH2M-Hill in the areas of infrastructure systems with focus on technology support for sustainable community lifestyles. This effort has brought focus on the intersection telecommunications, networking, and energy system infrastructures.

John has also been active in the Open Source movement through Open Commons and work with the GOSCON and Open Source Development Labs (OSDL). He engaged in early deployment of the Linux operating system (in 1994) and has worked with most major open source systems either in experimentation or deployment modes.

John was the founder and CEO of First Step Research, a boutique research consultancy which focused on the evolution of technology. John was also founder and CEO of First Step Internet, a wireless Internet Service Provider (ISP) started in 1994 to bring community based Internet services to rural communities in North Idaho/Western Washington. The service provided on-ramp facilities and training to all Washington state Economic Development Councils (EDCs) through Project 509, providing the first Internet and information services state-wide to these groups.

Prior to First Step, John was founder and Vice President of Engineering at Gold Hill Computers. At Gold Hill, John was central to the development of Concurrent Common Lisp in collaboration with Intel and the U.S. Army. Prior to Gold Hill, John worked with Honeywell Information Systems and Hewlett Packard as a Software Engineer and Systems Architect.

John also served 7 years as an instructor in the Department of Electrical Engineering at University of Idaho. John has received a Masters of Science degree in Electrical Engineering from the University of Idaho and an bachelor's degree in Math from Idaho State University.