**Title:**

'Uppity Civilians' and 'Cyber Vigilantes'[1]: The Role of the General Public in Policing Cyber Crime

**Authors:**

Laura Huey
Department of Sociology
University of Western Ontario
Room 5401, Social Science Centre
London, Ontario Canada N6A 5C2
Tel: 1-519-661-2111 ext. 87689
Fax: 1-519-661-3200
Email: lhuey@uwo.ca

Johnny Nhan
Department of Criminal Justice
Texas Christian University
Scharbauer Hall
2855 Main Drive
Forth Worth, Texas USA 76129
Tel: 817-257-4274
Fax: 817-257-7737
Email: j.nhan@tcu.edu

Ryan Broll
Department of Sociology
University of Western Ontario
Room 5316, Social Science Centre
London, Ontario Canada N6A 5C2
Email: rbroll@uwo.ca

**Abstract**

The distributed nature of the Internet requires that security issues be addressed through collaborative efforts within and across various sets of public and private actors. Drawing on nodal governance theory, this paper explores one aspect of the role that the general public can and does play in the field of cyber-security: civilian policing of the Internet. In particular, we examine the motives and actions of regular citizens, who use their computer skills to identify, track and collect information on the activities of suspected criminal offenders. Whereas some groups use such information to engage in vigilante acts, the groups that we study work cooperatively with police, collecting information to pass onto criminal justice agencies. We suggest that these collectives and their members are a potentially useful, if under-valued, component of cyber-security networks.

**Keywords**

Cyber-crime; Internet; policing; security

[1] The title is based on comments taken from an online source and refers to names that others have used to describe the work of civilian policing group members.

**Biographies**

Laura Huey is the author of several articles on cyber-crime, policing and victimization. Her research has appeared in various international journals and two monographs (Negotiating Demands: The Politics of Skid Row Policing (2007) and Invisible Victims: Homelessness and the Growing Security Gap (2012)).

Johnny Nhan is an Assistant Professor of Criminal Justice. His research focuses on issues of cyber and high tech crimes, from online piracy to prosecuting cyber offenders. His first book, Policing Cyberspace: A Structural and Cultural Analysis was published in 2010.

Ryan Broll is a doctoral candidate in the Department of Sociology at Western. His dissertation research explores the phenomenon of cyber-bullying and parental, police and school responses.

**Introduction**

In 2006, a 64 year old grandmother in Berkshire with few computer skills and no background in police investigative work, made a shocking discovery. Lurking on the alt.suicide.holiday cyber-forum, she began to uncover information suggesting that an individual with the online username of Li Dao was luring vulnerable people into phony suicide pacts, then inciting them to broadcast their deaths over webcam so that he could watch (Hawkins 2010; Brown 2010). Armed with this knowledge, Mrs. Blay began to trail Li Dao's online activities. Through website archival searches and email correspondence with members of various online suicide groups, she learned that Li Dao was engaged in similar activities under the pseudonyms of Cami D and Falcon Girl (Brown 2010). When Mrs. Blay had amassed what she believed to be sufficient evidence upon which police could act, she contacted her local police department, but was turned away for a lack of interest in the case. Mrs. Blay refused to give up. While continuing to track Li Dao, Mrs. Blay made a fateful decision: she and a friend created an online persona – an individual with suicidal thoughts – in an effort to see if they could engage Li Dao directly (ibid). Their ruse worked, and they were able to acquire his computer's IP address, which then allowed for his location to be traced. Having been subsequently also dismissed by the FBI and the Ottawa Police Service[2], Mrs. Blay used the IP address information to convince the police in Li Dao's hometown of St. Paul, Minnesota to take action. After an extensive police investigation, St. Paul police arrested 47 year old, William Melchert-Dinkel, a licensed nurse and married father of two (Porter 2010). Melchert-Dinkel was charged him with two counts of aiding suicide (ibid).

[2] Another of Li Dao's victims committed suicide in her home in Ottawa, Canada.

Structural and cultural limitations upon traditional policing agencies have resulted in a security deficit in the online world (author 2008, author 2010). This security deficit means that many crimes occurring online go unreported or are ignored by law enforcement; and, as the example above clearly illustrates, police often remain disinterested and/or lack the resources to deal effectively with the multitude of cybercrimes (Brenner 2004; Goodman 1997). Securing cyberspace is not, however, a simple case of expanding the current paradigm of crime control by adding more police officers or providing greater resources. Rather, the distributed nature of the Internet requires that the security deficit in cyberspace be addressed through collaborative efforts within and across various sets of public and private actors, each with differential access to economic and other resources and forms of social and cultural capital (Brenner 2004; Wall 2007; author 2008).

In a previous examination of the distributed nature of cyber-policing, we drew on nodal governance theory to demonstrate how much of the policing work that occurs in the online world happens through collaborative relations between four sets of actors collectively termed 'nodal clusters' (author 2008). These groups of actors are loosely categorized as: *government* (including federal, state/territorial/county and local bodies and their delegates); *law enforcement* (the patchwork of international, national, state/territorial and local policing agencies); *private industry* (encompassing the variety of private enterprises) and the *general public* (referring to everyday citizens, either as individuals or as members of online groups). In the pages that follow, we draw on our ongoing research of the latter – the general public – in order to begin the process of sketching out the complex role that the public can and does play in the field of cyber-security. As we detail below, online collectives of everyday citizens have sprung up for the purpose of addressing the security deficit in cyberspace. Whereas some engage in what could easily termed

online vigilantism, other individuals and groups form voluntary *ad hoc* partnerships with law enforcement. Following Sharpe, Atherton and Williams (2009), we describe their activities as ‘civilian policing,’ a term used loosely in this paper to refer to forms of online collective action aimed at pooling resources in order to investigate online crime and report information to law enforcement.

To explore the phenomenon of civilian policing in cyberspace and its relation to larger issues of cybersecurity, we draw primarily on an analysis of textual materials posted by such groups and their members. This material is supplemented with information from interviews conducted with a member of a voluntary civilian online policing group and with public police officers who work in this field. Data from these sources allows us to examine not only the motives, actions and resources of civilian policing groups, but also the extent to which they can and do play a role in facilitating cybersecurity.

*A caveat*: this paper is drawn from a larger, ongoing study of civilian participation in online security. It is intended as a preliminary report of our findings, one that we hope will encourage other researchers to consider exploring this ill-understood aspect of security provision.

**Nodal governance and collective online action**

The nodal governance theoretical framework developed by Shearing and Johnston (2003) builds upon Manuel Castell’s (1996) work on social networks. Recognizing that policing is increasingly a distributed phenomenon involving associations between and across public and private actors, the nodal governance model treats these relationship as analogous to the network relations one finds within the online sphere.

Within a nodal security framework, the building blocks of any network are ‘nodes’ – individual actors[3] with a stake in pooling resources to pursue collective forms of security. Each node brings to the network their own forms of capital, including social or political connections, resources and technologies. Groups of interrelated nodes that share common features or concerns have been termed ‘nodal clusters’ (Drahos 2004).

Security networks are formed when nodes within clusters actively choose to pool their resources with other nodes in pursuit of a security goal (Burris 2004, Wood and Shearing 2007). To better understand this pooling of resource, Dupont (2004; 2006) has sketched out five forms of capital that play significant roles in the formation, structure, and relation of nodal networks: economic, political, cultural, social, and symbolic forms of capital. To illustrate, *economic capital* refers to the monetary resources possessed by a particular node or a node’s ability to procure. *Political capital* relates to a node’s ability to influence public policy and use government resources. *Cultural capital* is “the knowledge base possessed by a node that can be mobilized for security” (author cite). *Social capital* refers to a node’s ability to create and maintain mutually beneficial social relations with others. Lastly, *symbolic capital* is an intangible asset that is often associated with institutional legitimacy and, therefore, directs the other forms of capital. Each node within a given security network has access to, and will contribute to the network, varying amounts of these forms of capital. Altogether, these five forms of capital determine the overall structure of the security network and its capacity for achieving its security goals.

[3] Nodes can be public, private, or hybrid institutions and may include anything from police departments to private corporations to individual persons acting on their own behalf or in the public interest.

The nodal governance theoretical framework is especially valuable for understanding security in cyberspace because, quite often, “security is derived from a collaborative network of nodal clusters” (author 2008). In the digital world, it is generally acknowledged that multiple security stakeholders must work together to detect and respond to perceived online threats (ibid). Nodal security online, therefore, involves the strategic and functional channeling of capital and other resources; when a security concern is identified, nodes take action or report the threat to nodal partners capable of taking appropriate action (author cite). In contrast to traditional policing which is often seen as passive and reactive, members of security networks are expected to proactively address common security concerns. Shearing and Wood (2003), for example, argue that participants need to become “denizens”: groups of active participants that belong to a particular community and share social capital in order to create functional communal spaces. In the virtual world, such individuals and groups have been referred to as “netizens” (Hauben and Hauben 1997).

As noted, the cornerstone of the nodal security model is the concept of shared collective capital. We see the pooling of capital in relation to various forms of collective action by netizens. For example, Human Flesh Search Engines (*renrou sousuo yinqing)* is a phenomenon that emerged in China in 2006, when active Internet community participants tracked down a woman who had filmed and uploaded a video of herself killing a kitten with her high heels. This group’s activities began when one online community member posted, “I have no interest in spreading this video nor can I remain silent. I just hope justice can be done,” which elicited responses typified by a statement by another forum member, who stated, “Find her and kick her to death like she did to the kitten” (Downey 2010). Outraged members analyzed the uploader’s Internet Protocol (IP) address, video background setting, and even the purchase location of her shoes to

identify and find the woman in six days, which resulted in the woman losing her job and posting an apology online (Liu 2008). The combination of old fashioned “have you seen her?” messages distributed amongst the network of millions of Internet users, coupled with more high-tech resources of IP tracing and analysis, makes the public node a very powerful security asset that is currently underutilized by law enforcement.

One online community that has been synonymous with shaping Internet subculture and engaging in Internet vigilante justice is 4chan.org, known mostly for using their collective resources for mischievous activities. In 2010, forum members quickly identified a UK woman petting then throwing a cat into a garbage bin and harassed her until she required police protection (Kelly and Sheerin 2010). However, 4chan community members have also aided police. In a similar animal abuse case, an unidentified woman was filmed maliciously throwing puppies into a river. 4chan members mobilized and tracked down the woman by tracing the YouTube video account of the person who filmed the incident, tracing him back to the woman, and subsequently turned information to the police for her arrest (Popkin 2010). While 4chan members have occasionally partnered with law enforcement, their *ad hoc* relations are infrequent and not suitable for sustained security. Instead our focus in this paper is those individuals and groups who form collectives for the purpose of engaging in proactive cyber-policing, which they see as being in concert with the aims and mandate of law enforcement.

To illustrate what we mean by online civilian policing groups, we can point to the example offered by one of the larger groups that we studied: a volunteer community established to disrupt and deter potential pedophiles from engaging in using the Internet to communicate and prey on child victims. Members pose as potential child victims, gather information on the perpetrator, and turn the information to the police for arrest and prosecution. Community

members share information, tactics, and participate in training to ensure legally admissible information is collected. This group, like similar others studied, works exclusively with police and do not engage in direct vigilante activities. They also attempt to share a robust and sustained relationship with law enforcement, with information sharing agreements, offering training to officers, and participation in joint sting operations. While other groups have had some successes, one thing that makes this collective unique is that the group touts dozens of arrests and a one hundred percent conviction rate.

**Method of inquiry**

Our research examines voluntary associations of citizens engaged in proactive civilian policing on the Internet. We draw from data collected from two sources: 1. online textual materials (threads and postings from relevant online forums) and; 2. data from interviews conducted with members of public police agencies and a representative of a civilian policing group. To acquire this data, we conducted three separate sets of research tasks.

We began with an archival news search of incidents of civilian involvement with online policing activities was conducted. Using various Internet search engines, we identified three main types of groups, which can be categorized based on the nature of their online activity as:

1. ‘vigilantes,’ where retributive actions (hacking, harassment and so on) are carried out by members independently of any association with law enforcement,

2. ‘civilian police,’ who collect and relay information on actual or potential online crimes to law enforcement, and;

3. ‘hybrid’ organizations that do both.

Although each of these forms is important to a better understanding of the public’s role in facilitating forms of cyber-security, this paper is focused on the second type noted: those groups whose members engage in civilian policing activities for the purposes of passing information to

criminal justice agencies for the latter to act upon. Thus, we narrowed the scope of subsequent data collecting efforts to amassing online text from organizations which seek to work proactively with public police agencies.

We began an exploration of civilian policing groups and their members – in particular, their motives and cyber-policing activities – by conducting an analysis of online materials from relevant websites. To do so, we identified four such groups and then utilized a mixed-methods approach, which entailed first coding and then quantifying responses found in online posts. For example, to explore the motives of individual members of these collectives, message board communications from threads such as one entitled "What drove you to come here?" were selected. In the case of one group, this threaded discussion was pinned to the top of a message board, allowing members to continuously comment without being bumped from the front page. The contents of this thread were coded into categories identified by the researchers[4] (such 'parental concern' and 'former victim') and then quantified. Using discourse analysis, the threads were subsequently analyzed for their content meanings and how these meanings can be understood in relation to the nature of the phenomenon studied, the discourse of both computer mediated communications (CMC) generally, and the group's own unique modes of communication.

We then we contacted representatives of online collectives that engage in civilian policing efforts. Despite our best efforts, site administrators of such groups were unwilling to allow us to post a call for participation on their sites. In one instance, a site administrator agreed to facilitate contact with members, then produced one individual who agreed to be interviewed.

[4] As of the time of this writing, there are 243 thread responses, with 173 found to be appropriate for coding. Excluded posts consisted of congratulatory or clarifying remarks.

Subsequent contact with this administrator netted no further results. Thus, in total, we conducted one interview with a member of one of the more active online groups. To supplement this meager data, and to add a further dimension to the study, we also interviewed four police officers who work in three different U.S. public agencies on computer crime issues. The police officers interviewed each had experience of working with civilian policing groups. The questions in our interview guide centered on the following issues related to our research: member motives, member activities, and individual or collective resources, skills and knowledge. All respondents were assured anonymity and advised that appropriate steps would be taken to ensure the security of their data.

**Civilian cyber-policing collectives: Member motives**

In seeking to better understand the role of the general public in cyber-security, particularly in relation to civilian forms of cyber-policing, it was important that we consider actors' motives for joining and participating in a collective of this nature. To aid us in this task, we examined one of the largest of the online civilian policing groups, where we found a forum containing a thread in which members were asked why they joined.

Table 1: Variables for participation in message boards (N = 173)

| Reason cited | f | % |
|---|---|---|
| Television or other media sources | 90 | 53.3 |
| Help prevent others | 82 | 47.4 |
| Justice | 62 | 36.0 |
| Former victim | 44 | 25.4 |
| Parental concern | 33 | 19.1 |
| Relative/friend of victim | 18 | 10.4 |

Note. Rates reported exceed 100% due to multiple responses across categories.

Several common motives for joining the group were identified amongst message board participants. Of these, the most frequent was exposure to media programs or news stories related to online dangers. Indeed, over half of the forum members who participated in the thread cited the television show *To Catch a Predator* as generating initial interest. The popular reality television show features civilians acting as decoys by posing as potential child victims. Individuals expressing interest in meeting these fictive children arrive at a ‘meeting location’ where they are exposed and confronted in front of cameras. Not surprisingly, some outraged viewers decided to ‘do something’ about the issue, by getting involved with an online collective aimed at detecting offenders. For example, a typical forum member response was, “I came to this after watching [To Catch a Predator]. I was shocked by what I saw on that show.” Another poster expressed the same sentiment, stating, “Every time we watched that show, I always felt a strong urge to DO something, anything … so … I jumped on.”

In coding responses, what we found is that reasons provided for joining were not always mutually exclusive. Thus, for example, initial exposure to a television program or news report was often twinned with other, more personal, secondary reasons for joining, such as being a former victim and/or seeking to prevent others from becoming victimized. For example, nearly half of the forum members cited the desire to help prevent others from being victimized as a reason for joining. “If I can do anything to help prevent such terrible things from happening to others, I will be happy,” one poster stated. This rationale was often paired with the explanation that a poster had been victimized or had family members or friends who had been victimized.

Many members were drawn to online civilian policing in order to seek justice. In this area, one person’s response was typical of this category: “I really wanted to join in the pursuit of justice as far as protecting the well-being of children by working toward catching sexual

predators.” In addition, a small number of thread responders within this category (n=8) felt law enforcement and the criminal justice system were inadequate in dealing with the problem. One thread participant explained, “Combating online predators takes HOURS of sitting at a computer screen. There just isn’t enough manpower, Colonel. There are specialized units out there, but it’s still a numbers game. Hundreds of law enforcement versus thousands of predators.” Another lauded what she perceived to be the superiority of collective citizen action over other modes of response: “It is hard to imagine that this many people (with such hugely different opinions in every other aspect of life) can put together such an organized successful effort and never even see each other face to face. It’s a shame the government can’t be this well run.” For individuals in this latter category, they are sometimes driven to collective action through outrage generated by real or perceived inadequacies of the criminal justice system. One member is frustrated with perceived inadequacies of the legal system: “I struggle with understanding the birds-eye view of these individuals, seeing someone with a dozen separate charges and still free to live and work like the rest of us.” Still another offered the following reasons:

> I volunteered because I don’t feel like enough is being done to combat this. The internet chat scene is basically the Wild West and predators are not afraid of getting caught. I feel like the [law enforcement] bureaucracy across the nation is either underestimating the prevalence of the problem or just don’t take it seriously enough and I don’t think that citizens should stand on the sidelines on this particular issue and wait for someone else to handle it.

Many forum members also stated that they had been victims of sexual assault as a child. This experience often fueled their desire to help others and seek solace. For instance, one forum member who was sexually victimized at the ages of 10 and 13, felt an underlying guilt in not being able to prevent the victimization of a relative. This individual was consoled by another member:

> Initial poster: I recently found out that the member of my family who molested me raped his 5 year old daughter 2 months before I turned him in. I cried for 3 weeks because I felt like it was my fault, if I would have came and told someone earlier maybe he would have been in jail and not hurt that little girl like he hurt me.
>
> Responder: You are NOT to blame. The person who hurt you is vile and disgusting. You were being *victimized* by a person you should have been safe with. It is NOT your fault he hurt others.

Similarly, personal direct exposure to victims has led others to take action. We note that this forum contained numerous other threads in which former victims discussed their experiences. In board parlance these are known as “survivor threads.”

The concern over the possibility of victimization of their own children motivates many parents to join these groups. Many parents became aware of the possibility of victimization of their own children through television programs and other mass media products, which frequently depict innocuous-looking child predators preying on children from typical suburban neighbourhoods. For example, one member was motivated by anger and concern after watching one such television program:

> I saw on there a predator who went to the home of a "13" y/o girl. After his arrest, they found in his possession condoms, marijuana, duct tape, and rope. I became nauseous, angry, and some emotions I don't know how to describe…I went and looked at my 13 year-old daughter peacefully sleeping and decided I needed to do something to stop these demons

Several discussion participants stated that they were motivated by the victimization experienced by relatives or friends. These individuals expressed great understanding and empathy for victims. For instance, one member stated, “Sadly, I came here when I realized that the loss of a friend when I was thirteen was due to these idiots and I now want to make a difference.” Another thread participant echoed this opinion: “A friend of mine, an adult not a

minor, suffered some sexual abuse online until I helped her end it…I just think it feels like it's time for me to help with this in some way."

In short, citizen motives for joining civilian cyber-policing groups are varied. However, we can distill at least one common theme from the motives examined: it is important for community members that they transform virtual message boards into equivalent *communal spaces* where they can exercise collective efficacy, what we call "digital defensible spaces" (Nhan and Huey 2008). These spaces "induce people to exercise some degree of social control in environments where they live" (Garafolo and McLeod 1989: 327). This sustained security environment requires members to 'buy-in' as security stakeholders and participate in as the online equivalent of 'denizens,' ('netizen') or active participants within a security node (Shearing and Wood 2003).

**Member capital**

Individuals who join online civilian policing groups assist in promoting collective security goals through mobilizing the forms of cultural capital to which they have access. Indeed, in the forum postings just discussed, a number of individuals stated that they believed they had valuable technical and other skills that could be utilized to catch online offenders. One such member shares his story, stating, "The work I do for my day job has given me experience in, and tools for, conducting open-source intelligence research, and the stories on the news have been stacking up. With the Chelsea King[5] case, I finally reached a point at which I felt I had to do my part." Another skilled member echoes this opinion, stating, "I am a software programmer that specializes in Cyber Security. I have seen the work of this organization in gear and am very

[5] Chelsea King was a 17 year old Californian girl murdered by a registered sex offender.

involved from a spectator standpoint. Hopefully, looking to step up and volunteer to add some additional muscle towards the efforts."

Other assets that community members can bringing to a civilian policing group include legal expertise, trained sexual assault counseling, criminal justice knowledge and experience in dealing with sexual assaults, among others. For example, one individual specifically joined a civilian cyber-policing group in order to offer counseling services to victims:

> I'm currently pursuing my master's degree in rehabilitation counseling---essentially, once I'm certified I can do just about any kind of counseling. I feel that with my expertise I can be a valuable resource on this site and basically hope to share and exchange thoughts and knowledge with other members.

Perhaps the greatest resources that civilian policing group members have is time and their commitment to their cause. This point was emphasized to us in an interview with a senior member of one group who, when asked about the resources that volunteers bring, said: "they have time." In aggregate form, time as a form of capital that individuals bring to the community, becomes a valuable collective resource. Indeed, according to one site's rules, time and investment in the group and its activities is not only necessary, but mandatory for group membership: "You have to become a part of the community. How do you become part of the community? By visiting, posting and interacting on a good regular schedule." In order to participate in more important functions, such as acting as chat room decoys, members of one group have minimum time and postings requirements before they are eligible to be apply for consideration as a full-fledged community member. Site administrators for this group feel the vetting process serves two purposes. First, it allows administrators to stream individuals into appropriate roles. In most groups, the most prestigious positions within the organization are decoys and verifiers, individuals who pretend to be potential child victims either online or by

phone. This work is legally sensitive and requires extensive training provided by experienced group members. Members are often required to demonstrate their commitment by performing lower-level tasks, such as “Facebook Cleanup,” where volunteers scour popular social networks looking for registered sex offenders. Offenders’ friend lists are warned and the offender is then reported to Facebook administrators. Second, vetting is necessary to filter out potentially dangerous individuals. According to one administrator, “Child molesters visit the site also.”

**Mobilizing security assets for collective good**

The collective use of security assets depends on the differing mentalities and cultures of each community. The willingness to work with law enforcement is often dictated by the level of control set forth by community administrators and forum moderators. Loosely controlled communities, such as the 4chan image board, tend to form organic aggregates with subsets of individuals acting independently in an *ad hoc* fashion. The groups we studied were instead highly structured, with organizers acting as volunteer coordinators engaged in selecting and training members, as well as interfacing with law enforcement officials. While the goals of members of groups such as 4chan are many and varied, the goal of the latter groups’ members is to meet desired collective online security outcomes, specifically by mobilizing their resources in order to collect and proffer digital evidence of online criminal activity to law enforcement and/or private entities.

In relation to working with law enforcement, the groups we studied mobilize the time and resources that individual members bring to the group. Drawing on their technical resources (tracing IP addresses, investigations), trained members collect incriminating evidence and, in some cases, conduct joint operations (‘stings’) with law enforcement. A member of one group informed us that what volunteers collect is “digital evidence” in the form of “screen shots,

pictures and chat logs.” As in the case of Mrs. Blay, some volunteers also help law enforcement identify offenders and their locations.

In two cases, groups examined were seen to advertise the availability of their services to the law enforcement community, seeking wider engagement with the latter in terms of meeting common security goals. One site put the offer a follows: “If your [law enforcement] agency is interested in conducting a sting operation with [us] we will put this service to work for you at absolutely no cost. We provide our large volunteer base of trained chat decoys, underage sounding telephone verifiers, internet researchers, as well as our software and databases, all for free.” The site further states:

> Our policy is to work with law enforcement in every case. We’ve created the “Information First” program to interface with police in a smooth and unobtrusive way. Information First is very simple. If a law enforcement department, detective or agency wants the “Information First”, they email us, we speak with them on the phone, and work out the details of jurisdiction and what they’d like to see out of the chat-logs we do. Then, we make a note for the Contributors of where Information First contacts are, what areas they cover and how to get ahold of them. Contributors then work Information First areas and turn over the information, first, to the already-stated interested and proactive police contact in that area.

The online collectives examined also present themselves as offering a vital service to private industry. As an example of how one such group works with the private sector in generating enhanced online security, community members perform niche online security functions on popular social networks, such as MySpace and Facebook. Indeed the group began a social network ‘clean-up’ project in 2007, mobilizing community members to comb these sites, identifying known sexual offenders to MySpace or Facebook administrators. To date, efforts by volunteer members to rid these sites of sexual offenders are said to have resulted in over 13,000

accounts being deleted.[6] According to the group's website, "both companies have been helpful and responsive towards removing danger users from their communities." Another group was specifically set up to target corporations and other private entities that are seen by group members as harboring pedophile activities. In most instances they collect information on alleged pedophile activities on a website or forum and then present this information to site owners in order to shut down the activity. Referring to their campaign against registered sex offenders [RSOs] online, they acknowledged that they do also attempt to work with law enforcement in some instances: "We have reported these RSO's to Myspace, and when appropriate, local law enforcement."

**Differing perspectives on civilian engagement with online security**

> We had been contacted by police local to both Aztram AKA Spurling and The Night Raven AKA Brisson back at the start of the month. Both were arrested of child molestation and child pornography once the police were able to obtain a search warrant based off our information
>
> – civilian policing website, 2011.

In both interviews and in statements published on group websites, members of online civilian policing groups see themselves as offering a valuable service in the fight for online security. To demonstrate that value, they proudly announce each arrest precipitated by their membership. As an example, we note both the above quote, as well as the following examples taken from a civilian policing website:

> We are very happy that these two subhuman individuals have finally been made to pay for their horrible and atrocious acts. They represent acutely why we do what we do, to expose these long-term members of online pedophile Websites. We're very proud and pleased that our work was able to get police attention on these two individuals and that further abuse has been stopped. They are two of many, and we hope that cases like this will bring even greater police attention to

[6] Section 4.6 of the Facebook Statement of Rights and Responsibilities specifies that convicted sex offenders are banned from using its services. (*See* www.facebook.com/terms.php). The MySpace Terms of Use Agreement section 8.15 prohibits sexual exploitation of members. (*See* www.myspace.com/Help/Terms).

> our project so that the rest of these people can get the attention they so rightly deserve. Congratulations to our research team for another job very well done.
> When our researchers had identified [name deleted] who was posting on BoyMoment, they were taken aback at the graphic nature of his stories. This project deals exclusively with disturbing material, but even amongst the dirt we deal with, [name deleted] stood out. We contacted a great detective over in Sacramento, California. He wanted more information, we supplied it and they got a search warrant. Once they searched his abode, they found thousands of images of child pornography. [He] will now spend a lengthy spell in prison

Not only do group members see themselves as an important node in the global online security network, but they also believe that police generally tend to see their work in similar terms. This perspective is made clear in the words of a representative of one such group who said in an interview with us, “most police organizations are favorable to our work. Occasionally we have run up against one that is less than eager to work with us, or that takes the view that civilians shouldn’t be doing work like this. They are however few and far between, mostly we have been well received.”

Certainly there have been a number of published reports of public police organizations in the U.S. conducting joint sting operations of alleged pedophiles with members of civilian policing groups. A representative of one such agency, the Darke County Sheriff’s Office, justified working with one group on the ground that whereas his department was under-resourced, the volunteer group “provided us with 140 [suspects] they were chatting with after 10 days, with possibilities of showing up for a meeting. There’s no way a department five times our size could have done that” (Garrett 2007). Similarly, a representative of the Riverside County (California) Sheriff's Department, who has worked extensively with one such volunteer group, sees drawing on volunteer assistance as a “progressive” means of responding to the complex problems posed by cyber-crime (ibid).

Interviews with public police officers who work in the field of computer crimes reveal a slightly more nuanced picture of police attitudes towards the value of civilian involvement in fostering greater online security. One police officer interviewed stated of groups such as those we have examined here, “We have offers from time to time saying ‘we know how to do this, we know how to do this,’ we tell them ‘no thank you.’” When we asked for the reasons behind his organization’s refusal to work with civilian groups, he offered two. The first had to do with legal liability issues. As he explained, “Anybody that you work with, if you say ‘Ok, I’m going to work with you’ then you automatically have the same powers and duties that I do. That opens the city to way too much liability because you don’t have the same training and expertise that we do.” The second rationale was captured in the following exchange:

> Q: So, there’s nothing that [one of these groups] can offer you that you can’t do yourselves? Is that what you’re saying?
>
> A: Exactly.

Each of the police detectives interviewed similarly stated that they felt that the involvement of organized civilian policing collectives in investigating cases was unnecessary, as well as potentially problematic. Aside from raising concerns with respect to maintaining the integrity of a case, two police officers worried that members of such groups could place themselves within dangerous circumstances. To illustrate this point, one cited the scenario of “a person [who] doesn’t know what they’re doing is out there going in over their head and potentially endangering themselves or potentially endangering others just because they want to help.” They both agreed that “we don’t want you to go out there and be doing things you shouldn't be doing in the first place,” and thus while receiving tips is useful, investigating cyber-crime should be left to the police.

Despite the potential benefits that can accrue through distributed policing systems that draw on active civilian support, the police officers interviewed see public involvement in cyber-policing as something that should be limited to providing basic tips. Such a finding is hardly surprising given that police subculture is well known for its mistrust of 'outsiders' (Skolnick 1966; Manning and Van Maanen 1978). We see these views mirrored in the practices of some of the larger civilian policing groups, which 'hand over' their digital evidence to law enforcement with no or little expectation of reciprocity of information sharing. To be fair, though, police skepticism and unwillingness to harness civilian policing groups can be seen as somewhat understandable given the public's definition of 'justice' may not always be predictable or legal (witness the actions of groups such as 4chan), and that the goals of a group or its members may be dissimilar to the legal and other mandates of law enforcement.

**Advantages and drawbacks: Some concluding thoughts**

Our research suggests that the general public can be a significant partner to public law enforcement and the private sector in securing cyberspace. First, as a result of the distributed nature of the online world, community members from across the globe can serve as 'eyes' and 'ears' for detecting criminal activity. Second, the speed at which the public can gather information and mobilize the various forms of capital to which they have access often far outpaces even the best law enforcement organizations. Indeed, a U.S. federal digital forensics examiner told one of the authors that "it takes [our agency] about six months to investigate and prepare digital evidence; it takes the FBI around a year." Certainly, increasing amounts of digital evidence secured through lengthy investigations has in fact created a substantial backlog for digital investigators in the U.S. (OIG 2009). A third advantage of public involvement in civilian cyber-policing activities is that such individuals and groups are diverse and thus their members

have access to a broad range of capital, including members’ time and skills – a fact exemplified by the activities of groups such as 4chan.

Despite the apparent advantages of civilian involvement in the provision of security in cyberspace, a fact recognized by some police organizations, civilian participation in online policing is not universally viewed by law enforcement as a desirable activity. Indeed, interviews with police investigators suggest that police subculture remains a major impediment to increased nodal partnerships with civilians. While the police cite legal liabilities associated with civilian involvement in investigations as the main issue, the existence of “Information First” policies whereby civilian policing groups provide neatly packaged information to police agencies with no expectation of reciprocation or further involvement undermines such claims. Further, we note that an alternative claim made by cyber-crime officers interviewed – that they receive no significant value from much of the information provided by civilians – has been refuted in media stories by representatives of other public police agencies, citing civilian policing group actions as critical to various investigative successes.

It would seem, therefore, that although the general public can be a vital partner in the provision of security online, they are currently a much undervalued nodal cluster in the cyberspace security network. While it may be possible to overcome the first two barriers identified – issues surrounding legal liability and the perception that civilians add no value to the investigative process – through “Information First” type programs and increased education efforts, altering police mistrust of civilian efforts is likely to prove far more challenging. The police mistrust of outsiders is certainly not new or unique to the policing of cyberspace; rather, it has long been identified as an impediment to police-public partnerships. With that being said, some partnerships, such as Neighbourhood Watch and other public safety initiatives, have

proven successful. Moreover, a variety of initiatives led by the police but seeking the public’s help, such as Crime Stoppers and AMBER Alert bulletins, has become an important tool for investigators. The success of such programs offline, and a handful of successful joint sting operations online (Garrett 2007), increases our belief that online police-civilian partnerships may be able to overcome the roadblocks that currently prevent a greater utilization of civilian policing resources. It would seem, however, that a tragic event or substantial public outcry might be necessary to spur such a movement.

Although there has been an increased recognition among academics that a nodal governance framework may be beneficial for securing the vast realms of cyberspace, more research is required on the role of the general public as an ally in this security network, particularly given the cultural capital and other resources they possess. Three particular areas of research may prove beneficial when attempting to understand the value and viability of the public as a security ally. First, while we examined the extent to which civilian policing groups engage in collaborative forms of security provision, further research should consider the role, if any, that vigilant groups, such as 4chan, play in fostering security online and what the strengths and limitations of this role are. Similar studies should attempt to understand the role of hybrid organizations that engage in both active and passive forms of justice play in fostering security online. Second, we still have little knowledge of the formation and mobilization of these justice-oriented online collectives. To this end, future research might employ social movement theories in order to better understand the processes that give rise to their creation. Third, although we conducted some interviews with officers who have had dealings with online civilian policing groups, continued efforts should be made to further understand police attitudes towards these groups and how more fruitful cooperative relations could be developed. While we have identified

important gaps, or limitations, in the overall security network, continued attempts to understand how or if these limitations could be overcome would be especially helpful.

**References**

Bayley, D. H., and Shearing, C. D. (2001). The new structure of policing: Description, conceptualization, and research agenda. National Institute of Justice Research Report. Retrieved on April 18, 2011 from www.ncjrs.gov/pdffiles1/nij/187083.pdf.

Brenner, S. W. (2004). Toward a criminal law for cyberspace: A new model of law enforcement? *Rutgers Computer and Technology Law Journal, 1*(30).

Brown, B. (2010). Village Sleuth Unmasks US Internet Predator Behind Suicide 'Pacts.' *The Sunday Times* (online). http://www.timesonline.co.uk. Retrieved on February 28, 2011.

Burris, S. (2004). Governance, microgovernance and health. *Temple Law Review, 77*, 335-359.

Burris, S., Drahos, P., and Shearing, C. D. (2005). Nodal governance. *Australian Journal of Legal Philosophy, 28*(2), 297-324.

Castells, M. (1996). *The information age: Economy, society, and culture, vol. I: The rise of the network society* (2nd ed). Maiden, MA: Blackwell.

Downey, T. (2010). China's Cyberposse. *The New York Times* (online). www.nytimes.com. Retrieved on February 24, 2011.

Drahos, P. (2004). Securing the future of intellectual property: Intellectual property owners and their nodally coordinated enforcement pyramid. *Case Western Reserve Journal of International Law, 36*.

Dupont, B. (2004). Security in the age of networks. *Policing & Society, 14*(1), 76-91.

Dupont, B. (2006). Power struggles in the field of security: Implications for democratic transformation. In J. Wood and B. Dupont (Eds.), *Democracy, society, and the governance of security* (pp. 86-110). Cambridge: Cambridge University Press.

Garrett, Ronnie. (2007) Internet Watchdogs. Officer.com website. www.officer.com. Retrieved on September 12, 2011.

Goodman, M. (1997). Why the police don't care about computer crime. *Harvard Journal of Law and Technology, 10*(3), 466-495.

Hauben, M. and R. Hauben. (1997). *Netizens: On the history and impact of Usenet and the Internet*. Los Alamitos, CA: IEEE Computer Society Press.

Hawkins, B. (2010). The Suicide Watcher. Minnesota Monthly (online). http://www.minnesotamonthly.com. Retrieved March 2, 2011.

Johnston, L. and C. Shearing. (2003). *Governing security: Explorations in policing and justice*. New York: Routledge.

Kelly, J., and J. Sheerin (2010). The strange virtual world of 4chan. BBC News. http://www.bbc.co.uk. Retrieved on February 27, 2011 from

Liu, D. (2008). Human flesh search engine: Is it the next generation search engine? Paper presented at the 3rd Communication Policy Research, South Conference, Beijing, China, December 5, 2008.

Manning, P., & Van Maanen, J. (Eds.) (1978). *Policing: A view from the street*. Santa Monica, CA: Goodyear.

Office of Inspector General (2009). The Federal Bureau of Investigation's efforts to combat crimes against children. OIG Audit Report 09-08. www.justice.gov/oig/reports/FBI/a0908/chapter2.htm. Retrieved on Retrieved on April 18, 2011.

Popkin, H. A. S. (2010, August 31). Web video: Woman Throws Puppies in River, 4chan Tracks Her Down. MSNBC (online). http://technolog.msnbc.msn.com. Retrieved on February 27, 2011.

Porter, R. (2010). Amateur Sleuth Unmasks Male Nurse 'Who Encouraged Dozens to Kill Themselves Online' So He Could Watch. Daily Mail (online). http://www.dailymail.co.uk. Retrieved March 2, 2011.

Sharp, D., S. Atherton and K. Williams (2008) Civilian Policing, Legitimacy and Vigilantism: Findings from Three Case Studies in England and Wales. *Policing and Society*, 18(3): 245-257.

Shearing, C., and J. Wood. (2003). Nodal governance, democracy, and the new 'denizens.' *Journal of Law and Society, 30*(3), 400-419.

Skolnick, J. H. (1966). Justice without trial: law enforcement in democratic society. New York: Wiley.

Wall, D. A. (2007b). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research, 8*(2), 183-205.

Wasserman, S., and Faust, K. (1994). Social network analysis. Cambridge, UK: Cambridge University Press.