Digilantism

Abstract:

This paper explores the aftermath of the Boston Marathon bombing incident and how members of the general public, through the online community Reddit, attempted to provide assistance to law enforcement through conducting their own parallel investigations. As we document through an analysis of user posts, Reddit members shared information about the investigation, searched for information that would identify the perpetrator,s and, in some cases, drew on their own expert knowledge to uncover clues concerning key aspects of the attack. While it is the case that the Reddit cyber-sleuths' did not ultimately solve this case, or provide significant assistance to the police investigation, their actions suggest the potential role the public could play within security networks.

On April 15, 2013, two bombs exploded near the finish line of the Boston Marathon, killing three people – including an eight year-old boy – and injuring more than 170 others in a shocking event that captured the world's attention. What followed was one of the largest, most sweeping investigations and manhunts in United States history. The suspects were identified, and then located, as a result of one of the most coordinated, technologically sophisticated efforts by local, state, and federal law enforcement. For example, the investigation employed a variety of forensic and other technologies, including surveillance video, explosive and blood pattern analysis, and helicopters with infrared cameras. The pursuit ended four days later, with one suspect, Tamerlan Tsarnaev, killed by police, and the other, Dzhokhar Tsarnaev, captured in dramatic fashion.

A significant part of the aftermath of the Boston Marathon bombing was the convergence of police, citizens, and technology playing significant roles in a real-time hunt for the perpetrators (Montgomery, Horwitz, & Fisher, 2013). Alongside the official investigation led by law enforcement officials was a parallel investigation conducted by a growing movement of online sleuths, often referred to as cyber-vigilantes, or "digilantes." These groups, organically formed in *ad hoc* fashion, harness the power of collective knowledge and resources – 'crowdsourcing' (See Howe, 2006) – towards a common purpose. In the Boston Marathon case,

cyber-sleuths were pooling information and resources in order to assist the police in their criminal investigation of the bombing.

While the events in Boston mark a notable example of this activity, digilantes have been playing a growing role in online and real world investigations. For example, in 2014, outraged social media users helped Philadelphia Police identify and find suspects who brutally assaulted a gay couple by matching online Facebook profile pictures of people who checked in at the restaurant where the beating took place with surveillance video (Shaw, 2014). This example shows how Internet communities can serve as 'additional eyes and ears' of the police in an age where demands for efficient service with increasingly fewer resources are strained by new communications and analysis technologies (Marx, 2013). Despite its apparent growing value for police, citizen involvement in police investigations is not without controversy. For example, the question of whether public online assistance to police was considered a form of neighborhood watch or a dangerous witch hunt was posed when Internet hacking group *Anonymous* publicly released personal information ("doxing") on the wrong person suspected of bullying Amanda Todd that resulted in her suicide (Davison, 2012).

Analyzing patterns of public and private participation in online policing-related activities can give insight into the boundaries of active and passive security roles in the new security framework that has emerged in cyberspace (author cite). To help flesh out the workings of this framework, within this paper we utilize data collected from Boston Marathon bombing threads in a popular online forum to examine efforts by members of the general public to identify and locate the perpetrators. Our analysis of member posts highlights the complex and nuanced role the public sometimes seeks to play in generating online-based investigations.

Digilantism

In the pages that follow, we begin by contextualizing the role of general public using the nodal governance theoretical framework, which views security as being distributed across a network of public, private, and hybrid institutions. Next, we discuss the research methods employed in this study—namely, data were drawn from an extensive review of more than 20,000 comments posted by users on the online community Reddit in the days after the Boston Marathon bombings. The discussion then turns to a presentation of the results of our analysis. Most users' posts were general comments about the event—expressing sympathy for victims and outrage at the terrorist attack—but others focused on sharing information about the attacks, such as personal videos and photographs. A smaller, but especially important number of posts aimed to support the ongoing police investigation. In these posts, users' shared real-time information about the investigation, scoured photographs and videos in an attempt to identify suspects, and used their own expert knowledge to identify key features of the attack. Although the success of the Reddit cyber-sleuths' investigation was limited (i.e., they failed to identified the bombers), the Boston Marathon attack was the first terrorist event in American in which the powers of the Internet were harnessed in an attempt to advance a police investigation. Thus, we conclude by offering a call for greater focus on the role of the general public as a security node.

The varieties of online policing

The evolution of police has been historically demarcated into different eras that reflect distinct changes in their core function. Kelling and Moore (2005) construct three historic eras based on police mandates and functional priorities: the *political era* during the mid to late 1800s, where police focused on maintaining the social order that were often political in nature, the *reform era* during early to mid-20th century, which sought to eradicate corruption through adherence to law enforcement and a professional demeanor, and the *community era* from the 1970s onward, which maintains a crime control function but seeks community support and

engagement through community-driven crime prevention and problem-solving strategies. A fourth era of policing suggested by the authors can be described as the *information era* of policing. Driven by demands of the information age and urbanization with larger officer-citizen ratios since the 1970s, police officers have become "knowledge workers" who collect and process information (Ericson and Haggerty, 1997). Modern officers, for instance, access information from mobile data terminals during stops before exiting their vehicles to assess the potential risk of the encounter (Manning, 2008).

Despite incorporating information technology into their case management and investigative practices, police find themselves being unable to meet growing demands for service. New forms of crime created by the Internet, such as hacking, and the use of the Internet in traditional crimes, such as identity theft and cyberbullying, have outpaced law enforcement's ability to control crime. Thus, a series of private actors – ranging from individual citizens to large corporations – have emerged who singularly and collectively play a role in the provision of security online (Wall, 2007).

To aid conceptualizing the complexities of security provision – in both the online and 'real' worlds – a new model of security was introduced derived from Castells' (2009) concept of the network society, where information networks shape social structures and activities. The *nodal governance* theoretical framework is based on the idea of distributed security in a non-hierarchical network consisting of security actors, or "nodes." In computer network, a node is a point of connection to a network, where information can be shared or accessed. Nodal governance nodes are security actors (institutions and groups) that share assets and work collaboratively for security purposes.

Digilantism

Burris, Drahos, and Shearing (2005) describe nodes as having a set of four essential characteristics: (1) *mentalities*, (2) *technologies*, (3) *resources*, and (4) *institutions*, or structures in which nodes can mobilize resources, mentalities, and technologies (p. 37-38). These nodal resources are used to exert influence over a security network. Nodal influence in a security network is not equal, with some nodes exerting more influence than others. Dupont (2006) lists the types of resources (capital) as metrics that determine the influence of a node in a network: (1) *economic capital*, or the monetary resources of a node, (2) *political capital*, or ability to mobilize governmental resources, (3) *cultural capital*, or "actionable knowledge," (4) *social capital*, or social relations with other nodes and individuals, and (5) *symbolic capital*, or centrality of a node to represent the other nodes (pp. 97-104).

Nodes in any given network can include a variety of security actors, such as the police. Within the nodal governance model, police organizations are considered one node in a larger security network that may also include private policing organizations, hybrid public-private security firms, and members of the general public. This "plural" model of security democratizes once police-exclusive functions of security into shared responsibility and resources (see Wood, 2006). Power within the new networked model of security is diffused to each actor, some of which may exert more power than others. Police, for instance, sometimes exert substantial power stemming from their cultural and social capital of representing the "moral order" of society, and their symbolic capital related to their ability to mobilize state-sanctioned legitimate power and resources, including the use of deadly force (See Dupont, 2004; 2006).

The arrangement of security nodal networks can be established or ad-hoc and scalable. The London Metropolitan Police, for example, coordinated the 2012 London Olympics using a large-scale nodal security network that utilized public-private security partnerships and

ubiquitous surveillance (Bennett and Haggerty, 2011). At a smaller scale, security alliances can form between police and citizens. For example, one cornerstone of community policing, an operating philosophy still embraced by most departments in varying degrees today, is information sharing and partnerships with police and citizens.

Perhaps the newest form of police-citizen collaboration is the use of social media by police. Some departments today are engaging the public through social media sites, such as Facebook and Twitter. The nature of these interactions, however, have reinforced the traditional model of police as knowledge brokers, in that social media serves mainly as a means of disseminating information and collecting information rather than engaging in public discourse. UK police forces, for instance, have used Twitter merely to supplement current channels of communications such as public service announcements and public requests for supplemental pictures and videos to aid in their investigations (Crump, 2011). However, another use of social media by police involves 'crowdsourcing': distributing labor to a large group of people – over the Internet – to achieve a particular task or goal that might otherwise tie up the resources of an organization. One example of such crowdsourcing in the policing world is public monitoring of CCTV systems over the Internet, which has expanded the surveillance capabilities in the UK as more eyes are placed on identifying suspicious activities and suspects (Trottier, 2014). Another example is the Vancouver Police Department's posting of images of individuals alleged to have participated in that city's 2011 Stanley Cup riots through a Facebook page, where visitors were invited to report anyone they recognized (Schneider and Trottier 2011).

While these forms of citizen engagement in online policing-related activities have attracted some researcher attention, the phenomenon of digilantism or 'civilian online policing' (authors cite) has yet to generate significant interest on the part of researchers or the police. As

we demonstrate in the analysis to follow, this lack of enthusiasm on the part of police agencies, does not place a damper on some citizens' desires to get involved online as 'eyes and ears' for the police.

Method of inquiry

Threaded discussion analysis was chosen as an appropriate measure of sentiments and collective action following the Boston Marathon bombing based on previous studies of communications within online groups (Malesky and Ennis 2011; Van Hout and Bingham 2013a; 2013b; the authors 2014). During the Boston Marathon bombing, users of the popular online community Reddit, created a number of Boston Marathon themed posts, titled "Boston Marathon Explosions: Live Update Thread #_" (labeled 1-21) to discuss the event in real-time. A main series of 20 continuous discussion threads were created as the unofficial forum for the site from the time of the bombing on April 15, 2013 to the capture of the suspects on April 20, 2013. Note that the researchers excluded thread 21 from coding, which was created after the official capture of the suspects and contained mainly congratulatory comments.

When each thread was determined to be too large by site moderators, the thread would be locked for further comments and a user would create a continuation of the thread (i.e., the next numbered thread from 1-21). In each thread, anonymous users made thousands of comments, ranging in nature from general opinions of the event to in-depth analysis of the bombings. A substantial amount of "popular comments" were automatically opened by the site for viewing without clicking for further comments. Top comments were voted on by community members, who can indicate whether a comment is good or bad by clicking on an up-arrow or a down-arrow. The threads contained an average of 1,034 popular comments (excluding responses to

these comments) and, in total, the researchers examined and coded over 20,000 anonymous user comments.

Two researchers independently coded the popular comments in each thread using a thematic analysis approach, and then cross-checked the coding for accuracy. Themes in user posts were initially identified through open coding, creating a total of 20 thematic categories. These categories included: 'support for victims', 'investigation-related information' and 'media criticism,' among others. These themes were solidified, and appropriate sub-themes identified and linked, through a second, more focused coding. The results were then analyzed in both qualitative format and using descriptive statistics. As our focus in this paper is on the role that the public played in trying to assist police in identifying and locating suspects, for this paper we draw primarily on our analysis of the theme of 'investigation-related information.'

Overview of results

Reddit threaded discussion data revealed several main categories in which users participated in the online discussions. First, the vast majority of participants simply used the forums as a means of self-expression. Second, participants sought to share and distribute news and other information, including a small number of Boston residents that provided real-time information from the scene. Third, some users offered direct or indirect assistance, such as offering to drive others to another location or offering up spare bedrooms to stranded visitors or family members of victims. Fourth, a group of users discussed topics directly related to the ongoing investigation, which included efforts at analyzing available information in order to identify and assist law enforcement in apprehending the suspects.

Table 1

Nature of Comments

Nature of Discussion	N	%
General comment	14,539	94.0
General question	572	3.7
Criticism of mainstream media	262	1.7
Seeking specific information	85	0.5
Racist comment[a]	14	0.001
Total	15,472	100

[a]Most racist comments were deleted by moderators or buried by users through down-voting.

Table 1 shows the majority of comments (94.0%) were general comments about the event. These ranged from outrage at the terrorist act to words of sympathy for the victims. A smaller number of individuals (3.7%) asked general questions, such as for updates or facts about the event, or sought specific information, such as how to locate a specific marathon participant.

A noteworthy number of forum participants (1.7%) criticized mainstream television news coverage, often while lauding the speed and accuracy of the Internet as a source of information. On the contrary, mainstream news outlets were strongly criticized for sensationalism and inaccuracy of information. For example, one community member typical of the message board sentiment as indicated by 163 "likes" by community members, expressed,

> On this note, don't listen to a word the NY Post says in regard to these explosions. Not that you should anyways. They have been sensationalizing and implicating racial connections where there are simply none known yet. (i.e., 'A 20 YO [year old] Saudi national is currently being detained in a hospital as a suspect'. This is bullshit, police have called them out on it).

A very small number of individuals (0.001%) made racist comments, usually by linking the terror suspects to Muslim or Middle Eastern ethnicities. These comments were quickly deleted by forum moderators or buried by forum users, who were quick to sanction the statement as being ignorant. Note that deleted racial comments were indicated by replies to the comment that sanctioned the comment for being racist. These comments are user-reported to forum

moderators and administrators. This process shows the self-regulating nature of message boards, and is not altogether surprising. Indeed, research has shown that people tend to distance themselves from those who do not align with their moral beliefs (Skitka, Bauman, and Sargis, 2005), and self-policing has been observed elsewhere in online communities (e.g., see Wall and Williams, 2007 study of Second Life and other virtual communities).

The public node of Reddit users acted as a real-time information hub (see Table 2). Of discussion posts involving the sharing of information, a large number of users submitted news links from traditional news outlets (29.8%), such as large television networks and newspapers, prompting many to forgo watching television news and, instead, obtain information from the board directly. Many users also listened to police scanners and emergency broadcast channels (19.1%), and were thus able to provide information to members of the online community before news outlets reported the same information. In addition, a smaller number of community members present in Boston submitted photos (16.0%) and videos (3.2%) taken themselves.

Table 2

Discussions Related to Information Shared Combined Threads

Type of Information	**N**	**%**
Boston users' news	162	4.4
Photos	592	16.0
Videos	120	3.2
Direct news link	1104	29.8
Secondary news link	1023	27.6
Hearsay news/police radio	708	19.1
Total	3,709	100

Public security assets

An analysis of the threaded discussions reveals unique security assets held by the public. The distributed and open nature of public forums, such as Reddit, attract individuals from a variety of professional backgrounds and interests. Whereas most law enforcement must cultivate

and develop its expertise from within its ranks to tailor to emergent crimes, such as cybercrime (see authors, 2010), or rely on small specialized sub-units within federal agencies economic and white-collar crimes, such as the FBI and IRS (see Friedrichs, 2010), members of public forums are professionals in a wide range of fields, which include IT professionals and accountants. In fact, Reddit's site contains sub-forums dedicated to specific interests that range from financing and computer security to religion and politics.

We see this wide variety of skills and expertise put to use during the Boston Marathon bombing investigation on the Reddit forums. In one post, a member claiming to have a background in military forensics gives detailed information on explosives and explosives investigations, stating:

> There are dozens of different ways to make explosives, and they all involve specific and well known chemical mixtures. You can perform a range of tests from the size and severity of the blast and burn marks on materials, to chemical traces on the ground, right through to chemical traces on the shrapnel. It's also very common for home made devices to explode in an incomplete or inefficient fashion, leaving traces behind. You are also quite likely to find evidence of the detonating device. How this is made and triggered (it can even have finger prints on it) is a huge clue.

The member goes on to explain the investigative steps and methods in great detail in relation to the explosives used in Boston. Similarly, another forum member claiming to have a professional background in explosives states:

> From the couple of reports I've read about what remnants were recovered, I think the devices were possibly crude DTMF (dual tone multi frequency) triggered devices. Without seeing the top of the circuit board that was pictured in the Daily Mail pic dump, I can't be sure. Anyways, this would lead me to believe that the devices were RCIEDs (Remote Controlled Improvised Explosive Devices), rather than a device that was triggered by a mechanical/electrical/chemical timer…Source: my field of work involves devices like this. I've seen a lot of them.

Underscoring the variety of expertise on the forums, other members in unrelated fields find themselves to be useful during the unofficial investigation. One forum member who is a

radio-controlled (RC) car enthusiast was able to help identify the triggering mechanism used in the bombing. He stated, "I am an RC modeler and one of the chips in the photos looks similar to ones use for RC cars. Shared my ideas here: [link to sub-reddit forum]." More remotely, a member working for a tire distributor found himself useful when trying to identify the suspect with the hat worn by one of the bombing suspects. He responded to a picture by stating:

> Hmm I work for a Tire Distributor and you get this hat for free for completing their Bridgestone "procert" testing. I actually have one in the mail on the way right now. I'm sure there's other places you can buy them but I just thought I'd throw that out there.

He was urged by forum members to quickly report his findings to the FBI. While these members' claims cannot be verified in terms of their expertise and represent only a small number of individuals (n=16) in our dataset, information shared can be a valued security asset not only a technical standpoint, but from the diversity of the expertise, as shown by the proclaimed professional tire distributor.

The value of security capital that comes from online communities is not derived primarily from the few experts or professionals, but from the sheer number of lay members from a variety of backgrounds.

Cyber-sleuthing: Civilian investigations online

In the aftermath of the Boston Marathon bombings, many Reddit users assumed the unofficial role of cyber-sleuth by acting as participants in the ongoing law enforcement investigation. These civilian investigators worked to compliment the official investigation and manhunt by serving as an extra set of "eyes and ears" for law enforcement. Combing through hundreds of pictures and videos, when a Reddit user identified information that may be pertinent to the FBI or Boston Police Department, he or she was encouraged to report it to law

enforcement. At the same time, forum users discouraged other members from becoming too actively involved in the investigation, such as by actively pursuing suspects.

As shown in Table 3, in the days after the bombing nearly 1,500 threads were created to share information related to the ongoing investigation (89.3% of all investigation-related threads). Many other threads (4.2%) were devoted to sharing information about the suspected bombers. Most often, these posts attempted to identify the suspects from photographs of the crown and blast area. Participants in these threads often drew attention to suspicious persons in the photographs whom users believed may have been implicated in the bombings. For many community members, this meant perusing photographs and videos for potential suspects in order to find and piece together information that law enforcement may have missed. In one such typical post, a member commented:

> What seems really interesting to me is they are on the move away from where the first bomb was placed. Notice the Bright orange jacketed guy it the very top corner, against the barrier. He is cut off from the edge in the first photo but using him as reference you can see most of the people around him stay in the same location (Red hood, White hood, white cap2). In the next picture white cap and shiny blue are 35-40 people down from orange jacket and moving out of the enclosed space, towards the second blast location. Orange and most people around him seem to remain near the Netherlands flag...Looking at an aftermath photo, it seems like the bomb was place right in this very location, near the brick cobblestone stripe. It is as if he placed it down right after this pic was taken!

Similarly, forum members conducted a *virtual* crime scene investigation by combing through the details of many photos of the blast posted on the Internet. For example, in one typical post, a member states,

> There is a lot more debris on the ground in the second photo, its also hard to tell from so far away. Remember, different angles give different depths to objects, so that burn mark may be further to the right in the second picture.
>
> Edit: Actually, if you zoom in, it almost looks like some sort of light-weight debris caught in the tree fluttering at the exact moment of the picture being taken. I'm probably wrong, but it just caught my eye.

Digilantism

Oftentimes, when "relevant" information was identified, community members reported it to the police.

Table 3

Discussions Related to Investigation

Nature of Discussion	N	%
Investigation-related	1,439	89.3
Suspect information	67	4.2
Technical information	6	0.04
Expert knowledge	16	1.0
Law enforcement link	84	5.2
Total	1,612	100

Other users provided contact information or direct links to reporting by law enforcement (5.2%). A small number of users (1.0%) claimed to have expert knowledge in the type of explosive used and provided information on different technical aspects of the bombing (0.04%). For example, one discussion thread included a lengthy description and analysis of the type of pressure cooker used to create the bomb:

> Going off the other picture with markings...
> "6 L: (So maybe that means 6 Liters?)
> CE marking. - This means it was made 1993 or later and is sold in the European Economic Area.
> "UL Listed" marking. Though UL has lots of markings none of which seem to match exactly.
> Possibly a number relating to the UL certification, but I can't make it out. Ending in "77??
> "0 55/1.05 –ar"
> "SS 1.6 ba-"
> It's hard to make out much from the photo, but that may help in searching or at least verifying findings.

This post was followed up by numerous replies going into great detail about the pressure cooker. As a result of their cyber-sleuthing, Reddit users were quickly able to identify the brand and model of the pressure cooker. A similarly detailed thread focused on identifying the details of the suspected bomber's hat.

Digilantism

In addition, forum members performed informal background checks on every suspect presented by other users, law enforcement, or mainstream media. Often, users looked up information posted on social media sites on the suspected person and their friends. Many went as far as to look up their shopping history on Internet retail site Amazon.com. A very small number of members presented conspiracies on motives and government involvement, comments that were often quickly dismissed by others as untrue and speculative.

Conclusions

The Boston Marathon bombing incident was a pivotal moment in citizen participation in policing. It was the first time a large-scale terrorist investigation was concurrently actively conducted by an online community. The result of this was an ad hoc nodal network of various law enforcement agencies, emergency workers, and the general public managed via the Internet. While the general public, in this instance, was not successful in their efforts (e.g., several "suspects" were incorrectly identified), the Boston Marathon bombing shows the potential for the general public—or informal cyber-sleuths—filling several deficiencies in the law enforcement system by serving as a resource, communications, and news hub, or a forum for finding support, and serving as additional 'eyes and ears' for law enforcement. While the capital possessed by the law enforcement node is static, the general public's capital is more fluid and may vary based on the composition of the group of cyber-sleuths.

Data extracted from Reddit forum posts reveal several patterns among community participation that reflect a growing demand for the public sector as a valid security node. The acceptance of the public as an active participant in the larger security network by law enforcement, however, remains uncertain. Internet users, in the case of the Boston Marathon event, have shown that simply having more "eyes and ears" does not necessarily translate into

better effectiveness. Among several misidentified individuals as the bomber, Brown University student Suni Triphathi, was the target of a "witch-hunt" generated by Reddit users, resulting in an official apology by the site (Van Grove, 2013). Despite this negative outcome, Reddit is just one of many online communities that organically emerges when tragic events occur which serves many important functions. Moreover, it is indicative of a larger role social media plays in not just a forum for commenting on crime but as a medium for active participation as security stakeholders.

Regardless of their value, online communities of 'digilantes' are here to stay. The value of the general public as a security stakeholder has yet to be realized, with police reluctant to accept any active involvement in investigations as more of a liability than real asset (see authors, 2012). Whether the police ultimately accept the general public as a legitimate partner and stakeholder node in the overall security network that can be integrated into their security framework is still unknown. However, with the evolving distributed nature of crime in the information age, old models of geographically defined policing may need a more distributed model that includes the public, both as additional crime detectors and as potentially valued experts in specialized fields.

This research should serve as a preliminary examination of the potential of the public as a security partner in investigations led by mainstream law enforcement agencies. While it is a less than ideal model of research, it provides a snapshot of the of online digilante groups at the moment of the incident, revealing mentalities and actions that are reflecting of aggregates of individuals coming together for a common purpose. Future research should include other forums and the interaction between law enforcement and private nodes, perhaps employing Wood's

(2006) comprehensive methodical nodal mapping exercise that identifies assets and mentalities of each node.

References

Bennett, C. J., & Haggerty, K. (2011), 'Introduction: Security games: Surveillance and control at mega-events,' in C. J. Bennett & K. Haggerty (eds.), *Security games: Surveillance and Control at Mega-events*, 1-19. New York, NY: Routledge.

Burris, S., Drahos, P., & Shearing, C. (2005), 'Nodal governance', *Australian Journal of Legal Philosophy, 30,* 30-58.

Castells, M. (2010), *The Rise of the Network Society: The Information Age: Economy, society and Culture, Volume 1* (2nd ed.), Maiden, MA: Wiley-Blackwell.

Crump, J. (2011), 'What are the Police Doing on Twitter? Social Media, the Police and the Public', *Policy & Internet, 3*(4), 1-27.

Davison, J. (2012, October 22), 'Online Vigilantes: Is 'doxing' a Neighbourhood Watch or Dangerous Witch Hunt?' *CBC News*,
Retrieved from:
http://www.cbc.ca/news/technology/online-vigilantes-is-doxing-a-neighbourhood-watch-or-dangerous-witch-hunt-1.1132015.

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 & B. Dupont (eds.), *Democracy, Society and the Governance of Security*, 86-110. New York: Cambridge University Press.

Ericson, R. V., & Haggerty, K. D. (1997), *Policing the Risk Society*, Toronto: University of Toronto Press.

Friedrichs, D. O. (2010), *Trusted Criminals: White Collar Crime in Contemporary Society* (4th ed.), Belmont, CA: Wadsworth.

Howe, J. (2006), 'The rise of crowdsourcing', *Wired Magazine, 14*(6), 1-4. Retrieved from: http://archive.wired.com/wired/archive/14.06/crowds.html.

Kelling, G. L., & Moore, M. H. (2005), 'The Evolving Strategy of Policing', in T. Newburn (ed.), *Policing: Key readings*. Portland, OR: Willan.

Malesky Jr., L., & Ennis, L. (2011), 'Supportive Distortions: An Analysis of Posts on Pedophile Internet Message Board', *Journal of Addictions & Offender Counseling, 24*(2), 92-100.

Manning, P. K. (2008), *The Technology Of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*, New York: New York University Press.

Marx, G. T. (2013), 'The public as a partner? Technology Can Make Us Auxiliaries As Well As Vigilantes,' *IEEE Security & Privacy*. September/October. Retrieved from: http://web.mit.edu/gtmarx/www/marx-publicas.html.

Montgomery, D., Horwitz, S., & Fisher, M. (2013, April 25), 'Police, Citizens and Technology Factor Into Boston Bombing Probe', *The Washington Post*. Retrieved from: http://www.washingtonpost.com/world/national-security/inside-the-investigation-of-the-boston-marathon-bombing/2013/04/20/19d8c322-a8ff-11e2-b029-8fb7e977ef71_story.html.

Schneider, C., & Trottier, D. (2011), 'The 2011 Vancouver Riot and the Role of Facebook in Crowd-Sourced Policing', *BC Studies*, 175, 57-72.

Shaw, E. (2014, September 16), 'Philly Hate Crime Suspects Tracked Down by Anonymous Twitter Hero', *Gawker*. Retrieved from: http://gawker.com/philly-hate-crime-suspects-tracked-down-by-anonymous-tw-1635661609/all.

Skitka, L. J., Bauman, C. W., & Sargis, E. G. (2005), 'Moral Conviction: Another Contributor to Attitude Strength or Something More?' *Journal of Personality and Social Psychology, 88*(6), 895-917.

Trottier, D. (2014), 'Crowdsourcing CCTV Surveillance on the Internet.' *Information, Communication & Society, 17*(5), 609-626.

Van Grove, J. (2013, April 22), 'Reddit Regrets Role in 'Online Witch Hunt' for Misidentified Suspect', *CNET*. Retrieved from: http://www.cnet.com/news/reddit-regrets-role-in-online-witch-hunt-for-misidentified-suspect/.

Van Hout, M. C., & Bingham, T. (2013a), 'Silk Road, the Virtual Drug Marketplace: A Single Case Study of User Experiences', *International Journal of Drug Policy, 24*(5), 385-391.

Van Hout, M. C., & Bingham, T. (2013b), 'Surfing the Silk Road: A Study of Users' Experiences', *International Journal of Drug Policy, 24*(6), 524-529.

Wall, D. S. (2007), *Cybercrime: The Transformation of Crime in the Information Age*, Malden, MA: Polity.

Wall, D. S., & Williams, M. (2007), 'Policing Diversity in the Digital Age: Maintaining Order in Virtual Communities', *Criminology and Criminal Justice, 7*(4), 391-415.

Wood, J. (2006), 'Research and Innovation in the Field of Security: A Nodal Governance View.' In J. Wood & B. Dupont (eds.), *Democracy, society and the governance of security*, 217-240. New York: Cambridge University Press.