# Amateurish detectives or expert investigators?

## Analysing the use of sources by websleuths in online case solving discussions

Ayla Kolster
Graduation Thesis, August 2019
Media Technology MSc program, Leiden University
Supervisors: Bas Haring, Nina van der Knaap
a.kolster@umail.leidenuniv.nl

Abstract: Websleuths, or cyber detectives, are people that are part of an online community who try to solve crime collectively. Sometimes these people have skills or an expertise that they can use for their online investigation, but most often they are amateurs who spend their free time sleuthing the internet. There are mixed opinions about the competence of crowdsourcing solving crime. Some argue that websleuths, or any other amateurs, should not interfere with the task of law enforcement (LE). Others anticipate that LE could benefit from collaborating with websleuths in order to outsource investigations that involve considerable amounts of manpower and time. But, to understand how allegedly unprofessional websleuths are, we need to examine their investigation method in correlation to police's methods. This research looks at the website Websleuths.com, a forum where people start discussions on cases to try and solve them. We did a content analysis of ten discussion threads using a list of police sources (Gottschalk, (2009) "Information Sources in Police Intelligence"). We concluded that websleuths use more of the same open sources as the police uses for investigation, than that they use different sources. Overall, websleuths methods for investigation based on the sources they use are quite similar to the police's methods.

Keywords: websleuths, cyber detectives, investigation, police sources, content analysis

### Introduction

In the aftermath of the 2013 Boston Marathon bombing, a subreddit, which is a thread on Reddit.com, was created with the intention of finding out who the culprit was[1]. A witch hunt ensued where every attendee of the marathon who wore a backpack could be a suspect (Rieder, 2013). Unfortunately, this pursuit ended in several people getting wrongly accused by Reddit users. One of these 'suspects' was Sunil Tripathi, a man who was missing and, as it turned out, had already killed himself before the marathon (Wade, 2014). However, a few reporters had already spread his name outside of the confines of Reddit's thread, resulting in his family getting harassed and receiving numerous threats (Shontell, 2013).

Almost 20 years earlier, in 1995, a man was killed in a car crash in Virginia. His identity remained unknown until his case began circulating the internet where he became known as Grateful Doe, as he was found with two Grateful Dead tickets on him (Staff, 2015). Because a composite sketch of this man had gotten a lot of attention on several online detective websites, a former

[1] https://www.reddit.com/r/findbostonbombers/

roommate recognized him as Jason (Rogers, 2015). His last name was later discovered to be Callahan, when Jason's mother heard a broadcast about this person who had amateur sleuths so interested for years.

Websleuths, also called online detectives or cyber sleuths, are people that are part of an online community who collectively try to follow, discuss or solve real life cases. They have, like the two examples above, involved themselves with investigating thousands of crimes or real life mysteries. However, not all have such explicitly good or bad endings. Most people who join such a community do this for one or more reasons: they have been exposed to media coverage of a specific case, they want to prevent other crimes from happening, they seek justice, they are a former victim, they do it because of parental concern, or they are a relative or friend of a victim (Huey, Nhan & Broll, 2013). Not all members of websleuthing communities actively join in on the discussion, some are simply observing. But, those who do participate occasionally have skills or an expertise that can help with the investigation. Some individuals have technical skills that are beneficial for retrieving information, others have legal expertise, knowledge about criminal justice, or are trained in victim counselling (Huey et al., 2013).

## 1. Problem statement

This civilian policing (Sharp, Atherton & Williams, 2008), as websleuths' activities could be labelled as, is intended to turn over discovered information to law enforcement in order to enable the conviction of a suspect and/or give the victim's family closure. However, opinions are divided about the idea of a collaboration between law enforcement and websleuths. Though citizen participation is already a known phenomenon (Cornelissens & Ferwerda, 2010; Lee & Zao, 2016; Bervoets, Van Ham & Ferwerda, 2016; Schreurs, Kerstholt, De Vries & Giebels, 2018) and has proven to be effective (Baumann, Schultz, Brown, Paredes & Hepworth, 1987; Van het Ende & Van Veen, 2018), some are against civilians aiding police in their investigations. This opposition generally comes from police officers themselves (Huey et al., 2013).

One would assume that law enforcement can benefit from assistance in certain investigations that involve considerable amounts of manpower and time. Though, it might prove harder to alter the police's mistrust of civilian investigation, than it is to overcome the obstacle of legal liability issues and alter the impression that amateur civilians are useless during an investigation (Huey et al., 2013). However, we argue that a closer look at the investigation methods of websleuths might give people a better understanding of the degree to which those methods are similar to police's methods. This, in turn, could reduce the apprehension against amateurs getting involved with law enforcement.

However, as is expected, law enforcement agencies have access to a large quantity of information only available through sources requiring warrants or police authorization. Websleuths, on the other hand, will most likely only have access to open sources, which is publicly available data. Civilians have no legal considerations for gathering information from open sources, but law enforcers are regulated during open source investigation as it gives them access to a vast amount of personal data which could breach individuals' privacy (Koops, 2013). Though not everyone agrees that the "protection of the fundamental right to privacy" is at risk (Tosoni, 2018), police investigators need to be mindful when seizing open source intelligence. This is in order to prevent infringing constitutional regulations protecting communications and avoid "committing specific offenses relating to communications and data." (Sampson, 2017) In other words, civilians have an advantage

over law enforcement officers regarding the acquisition of open source intelligence, since they are not inhibited by any regulations. This is another indication that it is beneficial to do a closer investigation of the activity of websleuthing to get a better understanding of the potential of a collaboration with law enforcement.

In order to hold websleuths' methods against a law enforcement framework, this paper will analyse what sources online detectives use and compare them to sources used by police. As explained above, we are primarily focussing on open sources. Sources form a crucial part of an investigation for information gathering and finding evidence. Therefore, we will try to answer the following question: In what way are the sources websleuths use for investigation similar to the police's methods? We will conduct a content analysis of the website Websleuths.com, which is, as the name suggests, an online forum for websleuths. In particular, we will look at several different discussion threads on this website in order to determine the use of sources for their investigations. We hypothesize that websleuths use more of the same sources as police than that they use different sources. Overall, we suspect that people on the website Websleuths.com use some of the same sources the police uses for investigation, but will also use different sources because not all of the police's sources will be easily available to them.

First, an overview of existing literature is presented in the next chapter. Chapter 3 will focus on a description of the website Websleuths.com, followed by the methodology in chapter 4. Then, the results will be presented in chapter 5. Lastly, the final chapter addresses the discussion of the research and results, and features some suggestions for future research.

## 2. Literature review

As mentioned earlier, this research focusses on the concept of websleuths. However, to get a proper understanding of this notion, it is valuable to address corresponding concepts, or concepts that are often used concurrently. In the next literature review we will first present the notions of digital or cyber-vigilantism and civilian policing of cyber-security. These have both similar traits as websleuthing, but are also somewhat different in nature. Lastly, some literature on websleuthing will be discussed.

### 2.1 Digital vigilantism and cyber security

Trottier (2017) classifies digital vigilantism as privacy violation by people on the internet that surpasses online and offline boundaries and facilitates a parallel form of criminal justice. This process involves a mutual annoyance or anger towards a target, against whom others organize an act of retribution, often in the form of weaponized visibility (exposure). Targets are often people who have offended others by breaking the law or engaging in immoral activities.

Campbell (2016) did a case study of a digital vigilante who is a paedophile hunter. She uses both these terms interchangeably, which creates the assumption that digital vigilantism always, or generally, entails proactive 'hunting' of or interacting with child abusers. However, as is clear from Trottier's definition, digital vigilantism can be aimed at any person who others deem to be in deserving of retaliation. On another note, Campbell concludes that digital vigilantism enables the development of policing and allows us to think about how "policing can be elsewhere and otherwise."

Also, Garett (2007) wrote an article about civilian sleuth groups who work together with law enforcement to bring down child predators. He notes that the success of these operations,

particularly in terms of arrest numbers, is greatly influenced by the size of this civilian investigation group and the speed in which they accomplish things. Despite the greater efficiency of such a group compared to any police department, resistance from law enforcement is more common than approval for this citizen-police cooperation, according to him.

Next, Chia (2018) did a content analysis of press coverage in China, Hong Kong and Taiwan to understand how cyber-vigilantism is portrayed in the news. This study showed that news coverage positively represented the voluntary aspect of cyber-vigilantism and advocates the activity as a positive citizen-driven operation that can "effectively reinforce social norms and state laws." However, unwanted behaviour, such as disregarding people's privacy or harassing a target was less likely to be represented in the media.

Furthermore, Chang, Zhong & Grabosky (2018) studied citizens' contribution to cyber-security and concluded this can be a successful co-production. However, they also found that "self-helping" citizens have a tendency to take matters in their own hands regarding criminals and have a more extreme idea of punishment than law enforcers. The researchers argue that only activities of citizens' contribution towards cyber-security that correspond with the law should be encouraged. Actions of those that "test the limits of legality" should be strictly delineated.

To continue, E Silva (2018) examined whether cyber-security vigilantes conflict with criminal justice. She argues that people who use force in response to criminal activity on the internet can pose a threat to investigations of cyber-crime. On the other hand, she notes that cyber-security vigilantes should not be eliminated from the process of improving cyber-security, as they have a part in this. Similar to Chang et al., E Silva discusses that citizen cyber-security activities that are on the edge of legal responsibility should be circumscribed.

Lastly, Huey et al. (2013) argue that groups of civilians are accumulating to focus on "the security deficit in cyber-space." Thus, they researched the motivations people have for getting involved with cyber policing and interviewed a few police officers about cyber policing by the public. They concluded that police officers wanted only limited involvement of civilian policing despite the advantages the public can have on policing cyber-security. They argue that the thousands of people who jointly spend their time investigating the internet create an immense 'task force' that surpasses the size of any police force. Not only is the community's speed of gathering information faster than "even the best law enforcement organizations," but the diversity of such a group enables them to access "a broad range of capital," which includes time and skills of members. Because of this, Huey et al. stress the importance of further understanding police opinions on online detective groups and efforts need to be made to comprehend how a successful cooperation can be established.

### 2.2 Websleuthing

Myles, Benoit-Barné & Millerand (2018) investigated a websleuth collective on Reddit called RBI (Reddit Bureau of Investigation). This case study focussed on the group's system of communication. This system resulted in having the ability to regulate behaviour in order to keep users from violating the guidelines and maintain an anti-vigilante nature. Though the "development of discursive practices online" is not new or original in itself, Myles et al. emphasized in what way these guidelines are produced in this context and how they relate to it. They conclude that citizens gradually change into something different than victims, suspects, or witnesses of criminal investigations through the formation of novel roles during the creation of public safety.

Similarly, Nhan, Huey & Broll (2017) did a case study of the websleuth investigation of the Boston Marathon bombing on Reddit. They argue that these actions "suggest the potential role the

public could play within security networks." Though, as is clear from the introduction, the Reddit users failed to identify the correct suspects and this might bolster law enforcement's view on websleuthing. According to Nhan et al., police departments should be urged to establish programs and approaches in order to employ civilians as "crime detectors." Accordingly, police control or supervision of civilian websleuthing may produce more helpful information as well as diminish unfavourable outcomes. They add that future research should focus on other forums of civilian cyber-investigation communities.

To get a contemporary understanding of websleuthing, Yardley, Lynes, Wilson & Kelly (2018) analyzed the representation of websleuthing in news media. Deriving from this, they argue that the concept is more diverse than was thought of before. They note that the phenomenon of websleuthing has received a lot of attention in popular culture, but has not been researched as much by criminologists. Due to this, Yardley et al. propose to criminologists to try to further understand the "complex and diverse motives, choices, forms, activities, impacts and environments of websleuthing."

To conclude from this literature review, the three concepts cyber-security policing, digital vigilantism and websleuthing have a lot of similarities in terms of characteristics, potential and the need for further examination. However, websleuthing is more than simply the act of policing cyber-security. Though civilians might be part of a websleuth community for the purpose of making the internet a safer place, advancing real-life security and seeking justice is what websleuths primarily aim for.

Furthermore, from the literature discussion it seems there are communities or individual people who only engage in a somewhat passive form of investigation while respecting the law. On the other hand, there are those participating in digital vigilantism in order to actively catch suspects by interacting with them or to act out revenge. Several of the discussed researchers argue that it is important to promote the former and thus restrain groups that merge on the line of illegality similar to the latter. Therefore, we will try to get a better understand of how websleuths' activities fit within the legal framework and how they regulate their legality. As will be explained in the next chapter, the community on Websleuths.com have strong self-regulation when it comes to legality, transparency and privacy.

## 3. Websleuths.com

As mentioned before, this paper will present a content analysis of the website Websleuths.com. It is a community where people gather to investigate real (criminal) cases to try to collectively solve them. Its members are from all over the world. The site launched in 1999 and was bought by Tricia Griffith in 2004. Everything on the website is accessible to visitors, but only people who register as a member are allowed to post. Roughly 150,000 people are registered.

It is a forum type website, meaning that a member can start a thread about a particular case and other members can respond, thus creating a discussion. When a discussion thread becomes very lengthy with replies, generally around 1,500 replies, a new thread is created where the discussion can continue, usually indicated with the corresponding number behind the thread's title. In most instances when one particular case or topic has more than one discussion thread, it becomes a separate forum under which all related discussions are grouped. Then, these and other relevant forums are organized in larger forums by topic. For example, on the home page one can find the forum called 'Ongoing Case Discussion Forums', which houses all discussions about cases that are

not yet resolved, but are not cold cases either. In there is a forum called 'Timothy Bosma', which is the victim's name of the case, that has 206 threads with discussions, information, evidence and other related things.
The community on Websleuths.com takes interest in a variety of cases. Examples are:

- Murder
- Missing person
- Unidentified person
- Cold cases
- Other crime related cases

Furthermore, there are also discussions on various other topics, such as (convicted) serial killers, true crime documentaries and podcasts, court trials, etc.

Websleuths.com is different from other forum websites since it has an extended list of rules and guidelines. The following is included:

- Social media: Profiles of victims and suspects (as communicated by law enforcement) are allowed. Also allowed are public pages, but people's posts and comments on these pages are not. Profiles of family members and friends of victim or suspect, or most other individuals are not allowed.
- Freedom of speech: Members do not have an absolute right to say what they want. Posts that are intended to provoke conflict are forbidden and things that go against the beliefs and purposes of the community are not allowed.
- User accounts: Only one account is allowed per person.
- Victim friendly: Bashing or harassing victims is not allowed. Only when a victim's behaviour is relevant to a case are members approved of discussing it. This also counts for family and friends of victims and suspects. Members are not allowed to investigate them when they are not mentioned as a suspect by law enforcement. Only when personal information (including names) is released by the media or police are member allowed to post it.
- Referencing outside sources: When quoting a source, such as a news article or photo, a link must be included in the post.
- Copyright: Only 10% of the original text of a published source, such as news articles, is allowed to be posted in a discussion.
- Verified professionals and case insiders: Members that have special knowledge or expertise about a certain field, or are insiders of a case, such as family members of victim of suspect, need to be verified by staff. Otherwise, these members have to abide the general rules for posting, as stated above, and are thus limited in giving valuable (personal) insight or information.

The list of rules and guidelines continues further, including general rules that are expected on a forum website. However, for the sake of relevance we will leave it at this.

Websleuths.com has a team of eighteen staff members who regulate the website. They are entitled to ban members and delete or edit posts when going against the rules. Members who want to get themselves verified as professional or official insider have to contact the staff, who will decide whether that person deserves the status. According to the etiquette and information section in the website, "Administrators have the final say with anything in this community."

Though there are more online communities of civilian detectives, Websleuths.com belongs to the top mentioned cyber-sleuth groups, together with those on Reddit, 4Chan and Facebook. However, contrary to these other websites, Websleuths.com is solely dedicated to online sleuthing,

meaning that people visit this site exclusively for this purpose. Its distinction also comes from the community's considerate nature and strict protocol, which is not common on the internet. The fact that staff members govern the website, and is not just regulated by members, determines that the rules are actually administered and order is somewhat maintained. This allows the community to focus on its objective, without breaking the law, and prevent people from getting bothered by members' actions.

## 4. Methodology

We conducted a content analysis of discussion threads on the website Websleuths.com, using a list of information sources used by police (Gottschalk, 2009). However, since websleuths generally only have access to open sources, as opposed to law enforcement, categories that include sources solely accessible through warrants or law enforcement authorization were eliminated from this list. These include: interview by means of interrogation of witness or suspect; network by means of police informants; surveillance of a location by means of video camera or microphone, usually live; communication control, such as wiretapping; policing systems; exchange of intelligence information between law enforcement agencies; accusations of people filing a claim with the police; control authorities, such as stock exchange and tax authorities. Thus, the final list is as follows:

- Location
- Documents
- Observation
- Action (provocation and action to cause reactions that represent intelligence information)
- Physical material
- Internet
- Citizens
- Media

(Gottschalk, 2009)

### 4.1 Sample selection

Ten case discussions from the last ten years were selected to avoid encountering broken links and missing data. The selected threads had a minimum of 100 replies to ensure people were adequately involved in this discussion, and a maximum of 800 replies to limit the time needed to analyse the complete discussion. To make sure that the selected discussion threads were actual investigations of a case, we selected from the crime and missing forum, which include discussions about murder cases, missing person cases, unidentified cases, cold cases and other criminal cases. From this list, single discussion threads were scanned for starting date and number of replies.

### 4.2 Coding

Every thread that met the requirements was analyzed from beginning to end. The starting date, number of replies, title of thread and date of analysis was recorded. Every user post was read to determine whether there was a reference to a source. If so, it was documented in a text editor program. Later, they were categorized in a table according to the list above. Sources that could not be categorized under the existing list were labelled as 'alternative source'. They were analysed later in order to determine if they were a subcategory of a source or represented a separate category. When more of the same alternative sources were encountered, a new source category was created.

After analysing ten discussion threads, the results were summarized in a table, see figure 1. 1 means that the source was present in the sample, 0 means it was not.

## 5. Results

| | sample | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | total | total sources |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Police sources** | Location | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 | 72 |
| | Documents | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 | 30 |
| | Observation | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | Action | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | Physical material | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 9 | 37 |
| | Internet | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 | 326 |
| | Citizens | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 5 | 13 |
| | Media | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 10 | 325 |
| **Alternative sources** | Police | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 2 | 3 |
| | Unknown | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 8 | 54 |
| **Total** | | | | | | | | | | | | | 860 |

*Figure 1: table with coding results and total sources.*

As presented in the table (figure 1), 7 out of the 9 police sources were encountered during the content analysis. Only two sources, observation and action, were not referenced in any of the analysed discussion threads. 4 of the 7 encountered sources were present in all ten discussions, namely location, documents, internet and media. Physical material was used in nine discussions and citizens were referenced in half of the discussions. This means that more than half of the police sources were used in more than half of the discussion threads.

Two new source categories were added to the list, namely police and unknown. Police indicates that a member contacted a police officer for information, this was recorded in two discussions. It is understandable that this source is not included in the police's source list, because they produce the information of this source. Unknown sources were sources that we were unable to identify, due to a broken link, missing photo, etc. They were present in eight discussions.

The last column in the table presents the total source count. This is also shown in the chart below (figure 2). The sources that were used the most, internet and media, were used significantly more often than any of the other sources.

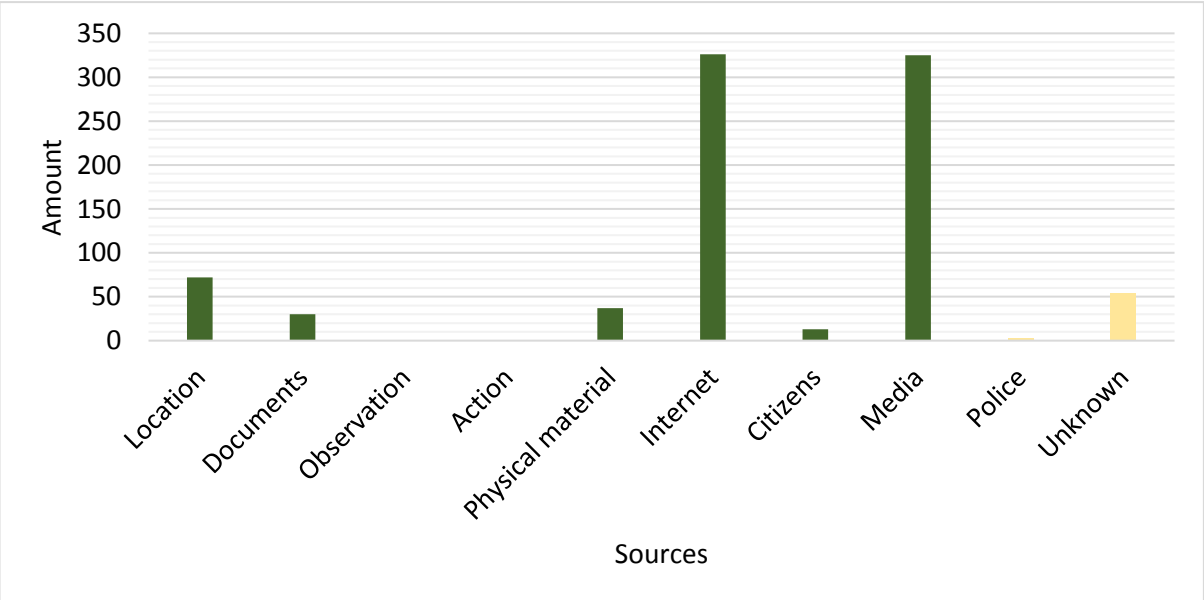


*Figure 2: chart with total source count.*

There were several other notable things we discovered on the website. First of all, people were noticeably civil and kind to each other. They respected others' opinions and tried to not offend other members. This is not at all common on the Internet. Furthermore, websleuths follow the rules and guidelines very strictly. For example, in a missing person discussion, the sister-in-law and friend of the missing woman wanted to join the discussion in order to provide insider information that was not available in any news sources. However, members cautioned them that they are not allowed to post any information without getting verified first. Otherwise, they needed to be able to link to the source of the information. Member JudgeJoe said the following after the missing woman's friend gave information about the boyfriend:

> *"I'm guessing you know Aubree's (the missing woman) boyfriend? If so, please consider becoming a Websleuths verified insider, so we can discuss the information you provide. Otherwise it is deemed 'rumor' and we can't consider. Another recommendation is to support the boyfriend in reaching out to mainstream media to tell his side of the story. It could help dispel false info and put pressure on law enforcement to find Aubree."*

Despite it taking a much longer time for the friend to get verified or contact the media than allowing her to post the insider information, they did this to minimize the possibility of false information in the discussion.

Also, websleuths are very careful to respect people's privacy. Personal information was only posted when that person was involved in the case and only after media or police had released their names. In one of those occasions, member *Shekkiec* said the following about the suspect: "Are we not allowed to reveal the name of her if it was on Facebook? Didn't want to break any rules." Member *FlossyMay* responded: "No. Police have not released that information to the public and it hasn't been mentioned in mainstream media." Members continued to refer to the suspect as 'her', or 'the aunt', as it was revealed in the media that the suspect was the victim's aunt. Much later in the discussion, someone linked a newly published news article were her name was identified. Only then, did a member post links to her social media accounts.

## 6. Discussion

The results indicate that our hypothesis is correct. Websleuths use more of the same sources as the police than that they use different sources. This means that their methods for investigation in regard to source use is quite similar to the police's methods. The reason why websleuth members use the internet and media the most is probably due to easy accessibility. The fact that websleuths did not use observation and action as a source to gather information, demonstrates that they are not cyber-vigilantes, or do not engage in any activity that resembles cyber-vigilantism. Furthermore, websleuths have a high regard for being civil, respecting privacy and avoiding speculation or false information. So, in our opinion, websleuths operate within the boundaries of the law and do not merge on the line of legal responsibilities. Therefore, in correspondence with Chang et al. (2018) and e Silva (2018), we argue that law enforcement should encourage websleuthing activities and pursue a successful cooperation with the Websleuths.com community. As Tricia Griffith spoke: "Can you imagine having a room full of people from all over the world that have all different types of specialties and not going to them for help? (Hitt, 2016)" We similarly agree that law enforcement agencies are seriously missing out if they choose to label websleuths as useless and unreliable.

Despite our efforts to conduct this research as scientifically sound as possible, it has some limitations. First of all, despite close reading and keeping track of coded sources, we could have miscounted several sources. For example, some sources were posted multiple times in a thread or some members that are actively involved in multiple discussions mistakenly replied in the wrong discussion. We were mindful of these errors, but some might have slipped and thus wrongfully counted. Secondly, in the case of ambiguous sources the coding relied on the coder's interpretation and comprehension to be able to get categorized. To test the coder's reliability, a sample was analysed twice with a few weeks in between. Both results were similar, but since it involved a small sample (a discussion thread of 139 replies) the test does not prove total reliability for bigger samples, where mistakes are more prone to happen. Therefore, the reliability of our findings is somewhat compromised.

Additional research is necessary in order to reproduce the findings of this study. A larger study with bigger samples needs to be done to confirm whether the results of this study are representative. Furthermore, this research did not focus on the differences in sources between the various discussion topics. It could be valuable to get a better understanding whether there is a significant distinction between murder case discussions, missing person discussions, cold case discussions, etc. Lastly, other online detective communities need to be subjected to a similar research in order to determine if they use the same sources as the police or have divergent investigation methods.

## References


- Baumann, D. J., Schultz, D. F., Brown, C., Paredes, R., & Hepworth, J. (1987). Citizen Participation in Police Crisis. Intervention Activities. *American Journal of Community Psychology*, *15*(4), 459–471.
- Bervoets, E., Van Ham, T., & Ferwerda, H. (2016). Samen signaleren. Burgerparticipatie bij sociale veiligheid. In *Platform31*.
- Campbell, E. (2016). Policing paedophilia: Assembling bodies, spaces and things. *Crime, Media, Culture*, *12*(3), 345–365.
- Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation and Governance*, *12*(1), 101–114.
- Chia, S. C. (2018). Crowd-sourcing justice: tracking a decade's news coverage of cyber vigilantism throughout the Greater China region. *Information Communication and Society*, 1–18.
- Cornelissens, A.; Ferwerda, H. (2010). Burgerparticipatie in de opsporing; een onderzoek naar aard, werkwijzen en opbrengsten. *Politie & Wetenschap*, *30*.
- Van het Ende, T., & Van Veen, S. (2018). 17 miljoen agenten. Burgerparticipatie in het veiligheidsdomein. In *Vertrouwen en wantrouwen in de digitale samenleving. Trends in Veiligheid 2018* (pp. 6–9).

- Garett, R. (2007). Internet Watchdogs. Retrieved August 20, 2019, from Officer.com website: https://www.officer.com/investigations/article/10249996/internet-watchdogs
- Gottschalk, P. (2009). Information Sources in Police Intelligence. *The Police Journal*, *82*, 149–170.
- Hitt, J. (2016). Social Justice: Tricia Griffith's Community of Internet Detectives. *Virginia Quarterly Review*, 12–17.
- Koops, B. (2013). Police investigations in Internet open sources: Procedural-law issues. *Computer Law & Security Review*, *29*, 654–665.
- Lee, J., & Zhao, J. (2016). Disentangling the myth about citizen participation in collaborative work with police. *Policing: An International Journal of Police Strategies & Management, 39*(1), 127-144.
- Myles, D., Benoit-Barné, C., & Millerand, F. (2018). 'Not your personal army!' Investigating the organizing property of retributive vigilantism in a Reddit collective of websleuths. *Information Communication and Society*, 1–20.
- Nhan, J., Huey, L., & Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston marathon bombings. *British Journal of Criminology*, *57*(2), 341–361.
- Rieder, R. (2013). Reddit Admits Missteps in Boston Fiasco. *USA Today*.
- Rogers, K. (2015). 'Grateful Doe' Is Identified 20 Years After Road Trip Death. *NY Times*.
- Sampson, F. (2017). Intelligent evidence : Using open source intelligence (OSINT) in criminal proceedings. *Police Journal: Theory, Practice and Principles*, *90*(1), 55–69.
- Schreurs, W., Kerstholt, J. H., De Vries, P. W., & Giebels, E. (2018). Citizen participation in the police domain: The role of citizens' attitude and morality. *Journal of Community Psychology*, *46*, 775–789.
- Sharp, D., Atherton, S., & Williams, K. (2008). Civilian policing , legitimacy and vigilantism: findings from three case studies in England and Wales. *Policing and Society*, *18*(3), 245–257.
- Shontell, A. (2013). What It's Like When Reddit Wrongly Accuses Your Loved One Of Murder. Retrieved August 19, 2019, from Business Insider website: https://www.businessinsider.com/reddit-falsely-accuses-sunil-tripathi-of-boston-bombing-2013-7?international=true&r=US&IR=T
- E Silva, K. K. (2018). Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting? *International Review of Law, Computers and Technology*, *32*(1), 21–36.
- Staff, C. F. (2015). How Internet sleuths solved the mystery of the 'Grateful Doe'. *Christian Science Monitor*.

- Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review*, *34*(1), 1197–1214.
- Trottier, D. (2017). Digital Vigilantism as Weaponisation of Visibility. *Philosophy and Technology*, *30*(1), 55–72.
- Wade, C. (2014). The Reddit Reckoning. Retrieved August 19, 2019, from Slate.com website: https://slate.com/technology/2014/04/reddit-and-the-boston-marathon-bombings-how-the-site-reckoned-with-its-own-power.html
- Yardley, E., Lynes, A. G. T., Wilson, D., & Kelly, E. (2018). What's the deal with 'websleuthing'? News media representations of amateur detectives in networked spaces. *Crime, Media, Culture*, *14*(1), 81–109.