Workshop 1 Ethics and Legal
Issues Inventory
Deliverable 4.1

Authors: University of Warwick & TNO

Co-funded by the Horizon 2020 Framework Programme of the
European Union
PLEASE NOTE THAT THIS REPORT IS A FINAL DRAFT AND IS AWAITING FINAL ACCEPTANCE BY THE EUROPEAN COMMISSION.


Report lead authors:

Kat Hadjimatheou (University of Warwick) and Arnold Roosendaal (TNO)
Contents

Executive Summary .................................................................................................................................. i

1. Introduction ....................................................................................................................................... 1
   1.1 MEDI@4SEC ................................................................................................................................. 1
   1.2 Work Package 4 ............................................................................................................................ 1
   1.3 Deliverable 4.1 (D4.1) ............................................................................................................... 1

2. Ethical and legal issues arising in connection with DIY policing initiatives ......................... 2
   2.1 Ethical Issues .............................................................................................................................. 2
   2.2 Legal Issues ............................................................................................................................... 4

3. Ethical and legal issues arising in connection with specific DIY policing platforms .......... 8
   3.1 Vigilante, Open 112 ................................................................................................................... 9
   3.2 Self-Evident ............................................................................................................................... 11
   3.3 Traffic Droid/Private Dashcam ................................................................................................... 12
   3.4 Digital Pillories .......................................................................................................................... 13
   3.5 Mafia Mapping ........................................................................................................................... 14
   3.6 Neighbourhood watch ................................................................................................................. 15
   3.7 Bellingcat ................................................................................................................................... 16
   3.8 Reddit .......................................................................................................................................... 17
   3.9 Opit, Stinson, Websleuths etc. ................................................................................................... 18
   3.10 Doxing ....................................................................................................................................... 19
   3.11 Crowd-sourced missing persons identification platforms ....................................................... 20
   3.12 Prey, Find my Smartphone ....................................................................................................... 21
   3.13 Policing the Police Apps ........................................................................................................... 22
Executive Summary

This report summarises ethical and legal issues raised in connection with citizen-led policing and security platforms that make use of social media. These issues were raised at the MEDI@4SEC ‘DIY Policing’ Workshop that took place on 9th Jan 2017 in Berlin, Germany. The workshop brought together 58 people, including police officers, researchers and citizen activists, to discuss digital citizen-led and citizen-influenced security initiatives.

The main ethical risks of DIY policing platforms identified in this report include: unjustified citizen interventions (vigilantism); overburdening of police with data; overburdening police with data whose utility is burdensome to verify; and disproportionate visitation of suspicion on individuals from certain social/ethnic groups. Benefits include: creation of a new model of ‘active citizenship’ and social responsibility; greater security for the public via preventive measures and better identification of criminals; and increased trust in police generated through co-creation of security. Key legal risks of DIY policing platforms include: disproportionate privacy intrusions; data protection violations; and vigilantism leading to illegal acts.

Specific recommendations arising from the discussion in the workshop include the following:

- Initiatives to educate people and enable cross-sector discussion and debate about the ethical and legal risks and benefits of DIY policing platforms should be pursued.
- Relevant authorities/collective organisations should seek to create and enforce a global digital policy.
- The visibility of LEAs in the virtual world should be increased.
- Best practices amongst social media platforms in reaction to grooming, bullying, etc. should be identified.
- Citizen perceptions and norms of self-regulation - their role and the role of platforms – should be studied to identify what is seen as legitimate.
1. Introduction

1.1 MEDI@4SEC

MEDI@4SEC focuses upon enhancing understanding of the opportunities, challenges and ethical consideration of social media use for public security: the good, the bad and the ugly. The good comprises using social media for problem solving, fighting crime, decreasing fear of crime and increasing the quality of life. The bad is the increase of digitised criminality and terrorism with new phenomena emerging through the use of social media. The ugly comprises the grey areas where trolling, cyberbullying, threats, or live video-sharing of tactical security operations are phenomena to deal with during incidents. Making use of the possibilities that social media offer, including smart ‘work-arounds’ is key, while respecting privacy, legislation, and ethics. This changing situation raises a series of challenges and possibilities for public security planners. MEDI@4SEC will explore this through a series of communication and dissemination activities that engage extensively with a range of end-users to better understand the usage of social media for security activities. MEDI@4SEC will seek a better understanding of how social media can, and how social media cannot be used for public security purposes and highlight ethical, legal and data-protection-related issues and implications. Activities centre around six relevant themes: DIY Policing; Everyday security; Riots and mass gatherings: The dark web; Trolling; and Innovative market solutions. MEDI@4SEC will feed into, support and influence changes in policy-making and policy implementation in public security that can be used by end-users to improve their decision making. By structuring our understanding of the impact of social media on public security approaches in a user-friendly way MEDI@4SEC will provide an evidence-base and roadmap for better policymaking including: best practice reports; a catalogue of social media technologies; recommendations for EU standards; future training options; and, ethical awareness raising.

1.2 Work Package 4

The role of Work Package 4 (WP4) is to identify ethical and legal issues arising from the use of social media for public security and policing purposes as well as to facilitate ethics procedures within the project. Ethics and legal issues will be reported for each of themed workshops.

1.3 Deliverable 4.1 (D4.1)

D4.1 Reports ethics and legal issues identified in the meeting: ‘DIY Policing - The Modern Sherlock’. Section 2 summarises the main issues that arose in the workshop discussion, while section 3 identifies issues arising in connection with the key DIY platforms that were presented during the workshop.
2. Ethical and legal issues arising in connection with DIY policing initiatives

In this section we report the cross-cutting ethical and legal issues that arose in the group discussion throughout the day.

2.1 Ethical Issues

2.1.1 The risks and potential benefits of a reinvigorated ‘active citizenship’

DIY policing initiatives were recognised in discussions as encouraging and enabling citizens to participate more actively in the maintenance of public security and that this is, on the whole, a positive development. For example, it was recognised that in some jurisdictions citizens are reluctant to engage in any way with police, mainly due to a lack of trust in policing. In places such as this, in which reporting rates are very low, DIY platforms can give citizens the option of reporting crimes fast and anonymously, thus encouraging increased cooperation with police. Similarly, on social media platforms, initiatives such as codes of conduct, reporting buttons, blocking features and ‘counter-speak’ can help discourage what was referred to in discussion as ‘voyeuristic participation’ - a type of participation where citizens observe certain forms of undesirable behaviour but they don’t act. It was recognised that DIY policing platforms can help to encourage - but also rely for their effectiveness on - a cultural change among platforms and their users. In particular, it was felt by some that the libertarian Internet culture should be replaced by a culture of active but responsible citizenship. DIY initiatives were seen as having the potential to extend trust in fellow citizens and the intrinsic drive to act that appears to exist in groups of citizens at a local level. In so doing, they can harness the (often detailed) knowledge citizens have of their local situation for public security ends. More active citizen participation in policing was felt likely to lead to citizen empowerment and eventually to a sense of improved security amongst citizens. Further expected benefits include the development of a sense of responsibility among citizens to abide by the law, as well a sense of value and connectedness among individuals within a society, adding to social capital. Greater education and awareness of as well as active involvement in generating ethical standards with respect to such initiatives were seen as vital to their effectiveness and their legitimacy.

On the other hand, concerns were expressed that enabling and even encouraging citizens to intervene in matters of crime and security via DIY platforms can risk fostering the notion that privacy is something that can be bypassed in the fight for criminal justice- for example, while searching for people involved in illegality, paedophile hunters “phish” sensitive information about people who are not doing anything illegal. Concerns were also expressed that widespread use of DIY platforms may increase suspiciousness and harm trust relations among citizens as people worry they are being mistakenly suspected of crimes or even maliciously identified as criminal suspects by other citizens. An increased risk of litigiousness among citizens was also cited as a concern. Finally, risks arising from discrimination-driven crime reporting
target selection based on social prejudice were cited as an area of concern, especially if platforms are used more frequently by members of certain social groups. Specific social groups may be overrepresented in interactions through social media while others may not take part at all or need further encouragement. It was felt that city government and polices should promote participation of minorities on the platform.

2.1.2 Risks and benefits to the legitimacy of police and local authorities

It was proposed in discussion that by enabling citizens to make a social contribution to policing, DIY platforms can bridge the gap between the police and the citizens and help provide more “legitimation” of police activities and practices in societies. This may be especially beneficial in jurisdictions in which there is mistrust towards authorities. The promise of improved transparency of government and police services offered by some platforms could also contribute to improvements in trust. Platforms designed to enable citizens to police the police are controversial, especially amongst LEAs, but even those participants felt that these were likely to lead to improved quality of policing and a more legitimate police force overall. For example, instead of pushing out their own story of a debatable police intervention, the police could pro-actively ask the public to upload their videos of the intervention, and make use of body cams to find facts and support their own story.

2.1.3 Overburdening of police with data

It was widely recognised that DIY platforms can help relieve some the work burden of LEAs by a) crowdsourcing intelligence and evidence from individuals, b) raising overall awareness on relevant issues (safety, privacy, etc.) among citizens and c) enabling citizens to deal with public security issues before they escalate to the extent that they require police intervention. However, worries about the potential for overburdening of police with data and demands for intervention both at a local and a national level were expressed, especially by police participants. There was a shared observation that local police work currently comprises a large variety of activities and multiplicity of tasks related to the maintenance of public order. In jurisdictions in which trust in police is high, civilians turn to them for support regarding all kinds of issues and incidents happening in public space, many of them unrelated to crime, because of the great visibility and popularity of the police forces. This was considered unfortunate, as it burdens police forces with petty incidents and a multiplicity of requests that could often be dealt with better by other public services. By making crime reporting easier and faster, DIY platforms might encourage even more over-reporting, or over-sharing of data with police. At the same time, they may encourage an expectation that reports will be dealt with by police; when that expectation is not fulfilled, this may undermine trust in and discourage use of the platform. As far as possible, DIY platforms should be designed with the need for information triage in mind.

A further source of burden for police arises from the difficulty of validating some kinds of citizen-generated data.
2.1.4 Need for education and new cross-sector forums in which ethical issues can be discussed and new standards accepted

Nearly all discussion groups cited the need for education on ethics online in order to develop the kind of culture in which DIY policing initiatives can pursue security effectively without undermining rights and values. Proposals ranged from education in schools and police recruitment colleges to the establishment of committees, roundtables and other kinds of forums involving local elected officials, police representatives, researchers, NGOs, community leaders etc. to discuss ethical and legal challenges pertaining to the use of social media in policing activities.

2.2 Legal Issues

As discussed in D1.3, DIY Policing raises a number of legal issues, depending on the technology or type of platform used. Discussion at the DIY Policing workshop in Berlin identified legal issues at stake and challenges and opportunities. Discussions were lively and diverse. Interestingly, the main issues were mentioned several times across the various round tables. However, at some points opinions diverged. This part of the report starts with a general overview of the legal issues and then connects these to a number of technologies that have been discussed during the workshop.

2.2.1 Ability of the law to keep up with technical change

One of the main issues raised in relation to the interplay between law and technology is that lawmaking is behind the facts. Technology moves fast and it would be of great benefit to all stakeholders if laws were able to keep up, both domestically and across jurisdictions. This does not mean that laws and regulations need to change every time a new app comes out. It does mean they need to be able to recognize the common cultures and features across apps and regulate those. For example, all apps harvest massive amounts of data (features); all apps that involve text boxes invite the same kind of communication (cultures). Police should recognize this too, and should be trained not to become confused by each new bit of technology. Even though this is a difficult issue, it was generally recognized that there is a need for more tech-savvy staff at LEAs, who are able to keep up with technological developments and can create a bridge between LEAs and DIY Policing initiatives. LEA presence and participation in social media platforms dedicated to DIY Policing is essential for good collaboration. And only with good collaboration can police ensure that DIY Policing initiatives enhance usual police work.

2.2.2 Legal clarity and understanding of the law

It was acknowledged that there is a need for proper knowledge of the laws related to policing and the use of social media in general. It is not always clear what exactly is allowed with regard to, for instance, the processing of personal data. The lack of knowledge or proper understanding has a few different undesirable effects. For example, in some cases, people working at LEAs are hesitant to share information, because they are afraid that it is not permitted in the law. This results in less effective use by LEAs of DIY Policing initiatives. Strikingly, during the workshop there were different viewpoints on this. Some argued that privacy laws make it very difficult to
share information and these laws should be changed, i.e. privacy concerns should be set aside in cases of information sharing about criminals or crimes. Others, however, argued that current laws are very well suited to protect the fundamental rights of everyone involved and still allow for enough options to share the necessary information. They indicated that the problems are more related to education and knowing what is allowed and what is possible, and not that the laws as such are too strict.

Many app developers or providers are unaware of the legal requirements for legitimate data processing. In addition, many of the users of apps are unaware as well, and in some cases it is easy and even encouraged to share as much information as possible. The lack of legal safeguards and professional oversight becomes problematic here. Since the professionals involved are not trained in the requirements for legitimate data processing, there is a risk that more information will be shared than is legally permitted. Data about people's suspected involvement in crime is categorized as sensitive data and their processing is essentially prohibited. Only under specific circumstances, such as a legal provision allowing an entity to process these data, or with the consent of the data subject, is processing allowed. Because of the applications, it cannot always be expected that there will be consent of the data subject, and non-professionals will not usually have another legal basis for the processing.

With regard to privacy, there is in fact a great opportunity at hand with the General Data Protection Regulation (GDPR), which will be effective from May 25th 2017 on. In the GDPR, present rights with regard to the protection of personal data are strengthened, and some new requirements are added. Particularly relevant in the context of social media use is the mandatory application of Data Protection by Design (DPbD) and Data Protection by Default. This means that all new forms of personal data processing activities have to be designed in a way that ensures the protection of privacy rights. New apps or information exchange systems that are developed have to take account of this principle. If DPbD is implemented properly, the risks of unlawful personal data processing are reduced.

There is a need for legal clarity on the admissibility of digital evidence in court. In particular, there should be greater clarity on how to collect and store digital evidence. If evidence is collected and shared, but cannot be used as legal evidence due to poor processing, e.g. with respect to the way it is stored, the benefit disappears. Some of the apps described below can help with this issue, but still it is very difficult to have a clear trail to verify the origins of digital evidence.

### 2.2.3 Lax approaches to data protection and privacy by vigilantes and citizen groups

Vigilantes tend to overlook or be unaware of legal provisions in place (they tend to know what is illegal but also tend to ignore the rights of the perpetrators, or they can have personal biases or interests). DIY policing can lead to intrusions in the privacy of suspected criminals, but also victims of crime. From a legal perspective, the correct balance between privacy and security must be maintained. So, there might be a need for education on legal aspects, perhaps by integrating legal and ethical training in school curricula. Other methods of training and education identified included public campaigns, and involving influential people who are peers of social media users, such a
vloggers. End User License Agreements (EULAs) can also help in obtaining consent and providing the right information to participants in DIY Policing platforms. Letting people know how to use the platform and what is allowed and what is not can be a major improvement. Without proper education and a good communication and interaction strategy, DIY paradigms can be a step back in the legal standards and how the law is applied with regard to ethical and legal issues.

The providers of DIY Policing apps have access to a great deal of content and personal data, and may be responsible as data controllers, in which case they must be compliant with data protection laws. Yet it may be difficult for them to monitor effectively and guide the way users process personal data when using the app. The processing of personal data by users includes processing of data about themselves, such as information on user profiles and account details, as well as data about (alleged) criminals. Currently, the processing of these personal data is not always arranged properly and in accordance with the law. For the processing of data of the users, there is often no proper informed consent. And for the processing of personal data about others, such as (alleged) criminals, there may be no legitimate ground as required in Article 6 of the General Data Protection Regulation (GDPR) at all. In a similar way, it is not evident that the basic principles from Article 5 GDPR are reliably or even typically respected. These include fair and lawful processing, data minimization, purpose specification (which can be an issue in individual cases), and storage limitation.

Participants/users of social media applications for DIY Policing do sometimes expose other individuals, such as (alleged) criminals. This exposure involves the sharing of personal data about these people. This can fall foul of data protection laws, which are intended to protect the fundamental rights of natural persons, notably their right to privacy (cf. Preamble paragraph 1 and 2 of the GDPR), by providing control over information being disclosed or otherwise processed. The impact can be severe. Not only can the amount of information sharing result in manhunts where people take the law in their own hands, and someone’s identity being made public, regardless of whether the person in question is really a criminal. Even if someone appears to be innocent afterwards, the damage to their reputation is very hard to undo or even limit, given the persistence online of accusations. It is still not clear whether the right to be forgotten (Article 17 of the GDPR) can be helpful in these cases, but it might provide the individual with the means to have online materials removed from search results at least (See the Google v. Costeja case of the ECJ). Legal safeguards, such as limited disclosure and verified quality and integrity of information, as applied by professionals such as police are not in place. Besides, even if the person whose privacy is infringed upon is indeed a criminal, this does not imply that the individual has forfeited all privacy rights.

Information shared online remains in the digital archives forever and this is an issue worthy of attention. Once posted online, information can be copied and shared and spread over the Internet. This is particularly likely in the case of information about (alleged) criminals. As a result, the privacy rights of people are infringed over a long time period and it is extremely difficult to get information removed to start with a clean sheet, even after someone has, for instance, been in jail after a conviction.
2.2.4 Cross-jurisdictional barriers

Next to the general problems surrounding the collection and use of digital evidence, cross-jurisdictional barriers are a real challenge to the pursuit of cyber criminals. Evidence procedures are barriers to using open source and other digital data to prosecute criminals. Moreover, it can be problematic if the police and DIY Policing actors across jurisdictions try to capture the same digital evidence and end up interfering with each other. The fact that someone is trying to collect digital evidence may also be detected by criminals, who may then block collection. It is, however, also possible that evidence becomes less reliable if different policing actors have accessed it and the logs indicate that it has been interfered with. Even though these problems are more of a technical nature, the result can be that judges consider materials unreliable because of this tampering (even if this is ultimately attributed to a lack of technical knowledge). The pursuit of criminal justice may in this way be undermined.

2.3 Conclusions and Recommendations

The following main takeaways from the workshop for future research and activities to improve the benefits of social media for DIY Policing:

- Initiatives to educate people and enable cross-sector discussion and debate about the ethical and legal risks and benefits of DIY policing platforms should be pursued.
- Relevant authorities/collective organisations should seek to create and enforce a global digital policy.
- The visibility of LEAs in the virtual world should be increased.
- Best practices amongst social media platforms in reaction to grooming, bullying, etc. should be identified.
- Citizen perceptions and norms of self-regulation - their role and the role of platforms – should be studied to identify what is seen as legitimate.
3. Ethical and legal issues arising in connection with specific DIY policing platforms

In this section we identify ethical and legal issues arising in connection with the specific platforms presented to the group at the start of the meeting. These are presented in bullet form in a table to enable easy reference for interested readers.
## Ethical Risks

<table>
<thead>
<tr>
<th>Legal Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vigilante has met with controversy and was removed from the App Store.</td>
</tr>
<tr>
<td>Apps enabling liveOPTIONAL - traceable emergency calls to be sent to members of the public as well as police and followed up on social media.</td>
</tr>
<tr>
<td>Legal risks include:</td>
</tr>
<tr>
<td>- Can prompt dangerous interventions (ones that multiply victimization).</td>
</tr>
<tr>
<td>- Can promote dangerous interventions that reflect preconceptions about who is suspicious and has criminal intent, causing wrongful suspicion to fall more frequently on certain groups.</td>
</tr>
<tr>
<td>- May be used in ways that reflect preconceptions about who is 'bad'.</td>
</tr>
<tr>
<td>- Can overlook police communications channels, making takes evidence.</td>
</tr>
<tr>
<td>- Licenses over-claiming and claiming that might not be useful/admissible</td>
</tr>
<tr>
<td>- Could encourage people to cut out police.</td>
</tr>
<tr>
<td>- Can encourage voyeurism, compounding victimization.</td>
</tr>
<tr>
<td>- Decide what a significant incident leaves to possibly attention-seeking, externalizing seeking users to</td>
</tr>
<tr>
<td>- The most obvious legal issue with these kind of technologies is</td>
</tr>
<tr>
<td>- Besides the rules of engagement within the app, there is the</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
| Vigilante, Open 217, 9

[3.1 Vigilante, Open 217](https://www.theguardian.com/technology/2016/nov/01/vigilante-app-removed-apple-store)
The mere fact that something is happening in a public place does not imply that sharing is allowed either. The reasonable expectation of privacy one has in a public place does not simply extend to alleged criminals being openly recorded. Even the police, who are allowed to process more information, are obliged to make a careful weighing of interests before making a picture or video public. The public access to these types of platforms and the way the videos are stored need to be considered carefully, taking the legal rules and requirements as guidance.

### Ethical Benefits

- Can provide evidence of criminal activities.
- Can rescue people.

### Legal Benefits

<table>
<thead>
<tr>
<th>Legal Benefits</th>
<th>Ethical Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Can provide evidence of criminal.</td>
</tr>
<tr>
<td></td>
<td>• Can rescue people.</td>
</tr>
</tbody>
</table>
### Ethical Risks

- Needs training to be used effectively and proportionately.
- Can encourage interaction with police from young tech-savvy people.
- Where trust in police and criminal justice systems is low.
- Would not deter serious, major, especially in communities of colour.
- If reporting is anonymous, can encourage people to report crime they have not witnessed.
- Can in principle provide admissible evidence.
- If not built in a way to be used effectively and proportionately.

### Legal Risks

- In order to be admissible as legal evidence, the footage has to meet certain criteria, such as a timestamp to indicate the moment of recording and an editing log to prove that the video footage has not been altered.
- Needs training to be used effectively and proportionately, which means they are collecting court-submissible evidence.
- May not be willing or able to get (ever someone could wrongfully believe). If the video evidence is used, it needs to be able to verify that the video was not fabricated.

### Ethical Benefits

- With in-built training, could be used effectively and proportionately.
- Can in principle provide admissible evidence.
- Can encourage interaction with police from young tech-savvy people.
- Can in principle provide admissible evidence.
- Can encourage interaction with police from young tech-savvy people.

### Legal Benefits

- Video and audio recordings can help in reconstructing the crimes or victims.
- Video and audio recordings can help in reconstructing the crimes or victims.
- Video and audio recordings can help in reconstructing the crimes or victims.
- Video and audio recordings can help in reconstructing the crimes or victims.

---

**Article:** Media4SeC  
**Grant Agreement no:** 760281

**Website:** https://www.witnessconfident.org/self-evident-app

**App enabling users to record, store, and share evidence and statements reliably and to file a police report from their smartphone:** Self-Evident

**3.2. Self-Evident

The Emerging Role of New Social Media in Enhancing Public Security**
Some road users are proactively recoding behaviour on the roads via cameras and other recording equipment in order to deter and capture evidence of traffic infringements. This article describes an extreme example of a London cyclist -

http://www.telegraph.co.uk/men/active/10851988/Traffic-Droid-the-cyclist-fighting-for-justice-on-our-roads.html

Ethical Risks:
- Processes without them knowing it.
- Processed without them knowing if or not, since many individuals can be filmed and have their data being processed without their knowledge.
- There is a privacy risk in the permanent recording by these applications regardless of whether there is a criminal act taking place.

Legal Benefits:
- Alternative to road rage.
- Can incentivize drivers to be more aware of cyclists and thus drive more cautiously.
- Alternative to road rage:
  - Less dangerous for cyclists.

Ethical Benefits:
- Alternative to road rage:
  - Can incentivize drivers to be more aware of cyclists and thus drive more cautiously.

Legal Risks:
- Reduction of hit-and-run accidents where the perpetrator could escape punishment or compensation to the victim.

Ethical Risks:
- Can generate more info than is usable by police.
- More justifiably used by professional drivers, for whom accusations of illegal driving may be a professional hazard.
- More justifiably used by professional drivers, for whom accusations of illegal driving may be a professional hazard.
- Can generate more info than is usable by police.

Traffic Droid/Private Dashcam

3.3 Traffic Droid/Private Dashcam

Grant Agreement No: 700281

The Emerging Role of New Social Media in Enhancing Public Security
The Emerging Role of New Social Media in Enhancing Public Security

3.4 Digital Pillories

This term refers to measures to name and shame lawbreakers online or on social media, as a means to deterring and punishing crimes felt to be

<table>
<thead>
<tr>
<th>Legal Benefits</th>
<th>Ethical Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>act on evidence.</td>
<td>Punishes (by shaming) rather than detects.</td>
</tr>
<tr>
<td>• Potentially justifiable if police are too busy with more serious crimes.</td>
<td>•</td>
</tr>
<tr>
<td>• Specifically case presented at the workshop - see link above!</td>
<td>•</td>
</tr>
<tr>
<td>• Apparently effective deterrent to crime (accordings to reports from the</td>
<td>•</td>
</tr>
<tr>
<td>• Could reduce future rates by prompting misconduct internally.</td>
<td></td>
</tr>
<tr>
<td>• Applications are often prohibited by data protection authorities.</td>
<td></td>
</tr>
<tr>
<td>• Since the infringement on privacy rights is significant, these kind of</td>
<td></td>
</tr>
<tr>
<td>• Place(s)?</td>
<td></td>
</tr>
<tr>
<td>• Courts usually consider a digital pillory disproportionate to its goals.</td>
<td></td>
</tr>
<tr>
<td>• Legal Risks</td>
<td>Ethical Benefits</td>
</tr>
<tr>
<td>• Legal Risks</td>
<td>•</td>
</tr>
<tr>
<td>• Ethical Benefits</td>
<td></td>
</tr>
</tbody>
</table>


Ethical Risks
• Punishes (by shaming) rather than detects.
• Potential justifiable if police are too busy with more serious crimes.
• Specifically case presented at the workshop - see link above!
• Apparently effective deterrent to crime (according to reports from the

graded

2 https://tweakers.net/nieuws/75941/cbp-digitale-schandpaal-wordt-zwaar-beboet.html

digitale-schandpaal-wordt-in-de-toekomst-zwaar-beboet.html
Mafia Mapping

**MafiaMaps** was a crowdsourced application enabling anonymous sharing of information about mafia locations in a city. Its development is currently on hold due to a dispute with the software developers.

### Mafia Mapping

**Legal Risks**

- Privacy and the right to be protected against violence.
- Open to malicious, inaccurate reporting.
- MISTAKEN or malicious reporting may lead to false accusations if people are clearly connected to individual locations.
- The anonymity of the application enables anonymous sharing of information about mafia locations in a city. Its development is currently on hold due to a dispute with the software developers.

**Ethical Risks**

- The anonymous aspect contributes to this. Open to malicious, inaccurate reporting.
- Malicious, inaccurate reporting.
- There is a risk of erroneous reporting of locations. Since anyone can indicate locations of the mafia, it is fairly easy to indicate wrong locations.

**Ethical Benefits**

- Gives up-to-date location information to police.
- Anonymity of the app allows people to communicate what everyone knows but cannot say, thus providing some form of community solidarity and resistance.

### Legal Benefits

- The anonymity within the application (or at least the visible maps)
- The availability of the app allows people to communicate what everyone knows but cannot say, thus providing some form of community solidarity and resistance.

### Legal and Ethical Benefits

- Mafia Mapping was a crowdsourced application enabling anonymous sharing of information about mafia locations in a city. Its development is currently on hold due to a dispute with the software developers.
- The application was on hold due to a dispute with the software developers.

### Legal and Ethical Risks

- Open to malicious, inaccurate reporting.
- Malicious, inaccurate reporting.
- There is a risk of erroneous reporting of locations. Since anyone can indicate locations of the mafia, it is fairly easy to indicate wrong locations.

### Legal and Ethical Benefits

- Gives up-to-date location information to police.
- Anonymity of the app allows people to communicate what everyone knows but cannot say, thus providing some form of community solidarity and resistance.
More (social) resources are made available for crime prevention.

Legal Benefits

- Proposed to reduce certain kinds of crime (e.g. burglaries in the areas-WhatsApp-neighbourhood-watch).

Ethical Benefits

- Can lead to surveillance of people who are not suspects but merely happen to be in the vicinity of recording equipment.
- Can be used for other personal vendettas.
- Can lead to suspicion being visited on people or certain social or ethnic backgrounds, resulting in people feeling pressured to join or seem suspect.
- Can lead to information-sharing way beyond security purposes.

Legal Risks

- Surveillance of people who are not suspects but merely happen to be in the vicinity of recording equipment on the property and garden.
- People who are not trained professionally in recognizing crime can misinterpret situations in their neighborhood, thereby unintentionally leading to wrongful accusations. The challenge lies in determining whether a situation is suspect or not. People have to be aware of what to pay attention to.
- Neighbourhood watch applications, people living in a neighbourhood are encouraged to be alert to criminal or suspicious activity and report it to others on the network.

Ethical Risks

- Neighbourhood watch applications, people living in a neighbourhood are encouraged to be alert to criminal or suspicious activity and report it to others on the network.

3.6 Neighbourhood watch

Grant Agreement No 700281

The emerging Role of New Social Media in Enhancing Public Security

MEDI@4SEC
The Emerging Role of New Social Media in Enhancing Public Security

Grant Agreement no 700281

3.7

Ethical Risks

- Impact on the capability of LEAs to enforce the law
- Legal Risks
  - Possible reduction of trust in police if Bellingcat publishes their results
- Ethical Benefits
  - Can provide reliable scrutiny of the accuracy of claims made by states

Legal Benefits

- There is cooperation with LEAs and evidence and materials are handed over to LEAs, helping investigations
- Can provide reliable scrutiny of the accuracy of claims made by states

Ethical Benefits

- Can provide reliable scrutiny of the accuracy of claims made by states
- Transparent methods enable counter-scruiting and thereby legitimacy
- Can lead to miscommunication and informal punishment rather than police apprehension

Ethical Risks

- Bellingcat’s role is to perform citizen journalist investigations in parallel with LEAs. It makes use of a large network of people involved and crowdfounding to solve parts of the puzzle,
- If investigations chosen by newsworthiness can lead to revision by criminals
- Legal Benefits
  - There is cooperation with LEAs and evidence and materials are handed over to LEAs, helping investigations

Bellingcat

https://www.bellingcat.com/
Reddit

A platform for user-generated content, where people can chat and share video and images.

<table>
<thead>
<tr>
<th>Legal Risks</th>
<th>Ethical Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggers by the content that have been uploaded.</td>
<td>Police apprehension.</td>
</tr>
<tr>
<td>There may be a risk of people taking the law in their own hands when privacy of people being exposed in the content.</td>
<td>Can lead to misidentifications and informal punishment rather than...</td>
</tr>
</tbody>
</table>

**Ethical Benefits**

- •

**Legal Benefits**

- •
Ethical Benefits

• May deter child abusers,

Legal Benefits

• Stands in several locations.
   • Can be copied and shared, and will be spread over the Internet and
   • Damage occurs from this. Online content remains online forever,
   • Controversy is posed online; there are hardly any options to repair the
   • Account that once there is an impact on privacy because defamatory
   • Account that once there is an impact on privacy because defamatory
   • Regardless of whether the target is indeed the criminal, the impact
   • Legal risks can be severe. Moreover, it has to be taken into

Ethical Risks

• Can harm methods of detection.
   • Online techniques can lead to entrapment.
   • When erroneous accusations are made online it may be very difficult
   • Legal Risks

Legal Benefits

• Can lead to prosecutions where relying on police would not be possible.
• Can lead to prosecutions where relying on police would not be possible.
   • May deter child abusers.

Ethical Benefits

• May deter child abusers.

Legal Risks

• Can harm methods of detection.
   • Online techniques can lead to entrapment.
   • When erroneous accusations are made online it may be very difficult

Ethical Risks

• Can harm methods of detection.
   • Online techniques can lead to entrapment.
   • When erroneous accusations are made online it may be very difficult

Legal Benefits

• May deter child abusers.

Ethical Benefits

• May deter child abusers.

Legal Risks

• Can harm methods of detection.
   • Online techniques can lead to entrapment.
   • When erroneous accusations are made online it may be very difficult

Ethical Risks

• Can harm methods of detection.
   • Online techniques can lead to entrapment.
   • When erroneous accusations are made online it may be very difficult

Legal Benefits

• May deter child abusers.

Ethical Benefits

• May deter child abusers.

Legal Risks

• Can harm methods of detection.
   • Online techniques can lead to entrapment.
   • When erroneous accusations are made online it may be very difficult

Ethical Risks

• Can harm methods of detection.
   • Online techniques can lead to entrapment.
   • When erroneous accusations are made online it may be very difficult

Legal Benefits

• May deter child abusers.
### Doxing

This is the sharing of usually identifiable information. The aim is to find individuals who have been accused of anything unlawful.

<table>
<thead>
<tr>
<th>Ethical Benefits</th>
<th>Ethical Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can be used as a form of self-protection for the cyberstalked.</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legal Benefits</th>
<th>Legal Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

**Legal Safeguards**, such as balancing of interests and opportunities to

- People attracted to these kind of initiatives are often thrill seekers;
- People that they become the victim of violence and manhunts;
- People that they become the victim of violence and manhunts;
- People that they become the victim of violence and manhunts;
- People that they become the victim of violence and manhunts;

- **Efficient Intrusion for the Aggressive Hacker**.

- **Ethical Risks**
### Ethical Benefits

- Reduces costs and adds manpower to investigations.
- To be successful on a wide scale.
- Ethical Risks

- If volunteers do not receive the guidance and training that is needed.
- The need for coordination of activities with higher conflict with the self.
- The need for coordination of activities with higher conflict with the self.
- If volunteers do not receive the guidance and training that is needed.
- The need for coordination of activities with higher conflict with the self.

### Legal Benefits

- These kind of applications can be used in a proper manner without will of the state.
- Very low-risk if run by police in a liberal jurisdiction (i.e., police whose role is to protect the human rights of citizens rather than enforce the law). Risks from police in a liberal jurisdiction (i.e., police whose role is to protect the human rights of citizens rather than enforce the law).

### Legal Risks

- Legal risks from police.
- The need for coordination of activities with higher conflict with the self.
- The need for coordination of activities with higher conflict with the self.

### Ethical Risks

- If volunteers do not receive the guidance and training that is needed.
- The need for coordination of activities with higher conflict with the self.
- The need for coordination of activities with higher conflict with the self.

### Ethical Benefits

- These initiatives recruit volunteers to help identify missing persons or solve cold cases. An example is the Doe Network—a US-based initiative to

---

**3.11 Crowdsourced missing persons identification platforms**

**Grant Agreement no 700281**
<table>
<thead>
<tr>
<th>Ethical Risks</th>
<th>Legal Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invites dangerous interventions.</td>
<td>If used widely enough may deter criminals.</td>
</tr>
<tr>
<td>Legal Risks</td>
<td>Ethical Benefits</td>
</tr>
<tr>
<td>These are pieces of software that help people find a lost laptop or smartphone. The app shows the location of the stolen or lost device.</td>
<td>Efficient stolen phone recovery if used for notifying police;</td>
</tr>
<tr>
<td>Prey, Find my Smartphone…</td>
<td>Can be a means of retrieving stolen goods (and therefore addressing a crime) that police may not pursue;</td>
</tr>
</tbody>
</table>

Prey is a means of retrieving stolen goods (and therefore addressing a crime) that police may not pursue; efficient stolen phone recovery if used for notifying police; if used widely enough may deter criminals.

Grant Agreement no 700281

The Emerging Role of New Social Media in Enhancing Public Security
<table>
<thead>
<tr>
<th>Legal Risks</th>
<th>Ethical Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can infringe privacy rights of those being filmed.</td>
<td>Can improve access to justice by recording wrongdoing for purposes</td>
</tr>
<tr>
<td>Ethical Risks</td>
<td>Legal Benefits</td>
</tr>
<tr>
<td>Has the potential to alienate the public from the police and vice versa.</td>
<td>Can improve accountability;</td>
</tr>
</tbody>
</table>
| Further entrenching  
Social assumptions and stereotypes. | Can deter police misconduct; |
| May create a negatively skewed impression of policing performance. | Can enhance accountability; |

3.13 Policing the Police Apps

https://www.aclu.org/feature/aclu-apps-record-police-conduct

These apps enable citizens to record interactions with police. Examples include the American Civil Liberties Union (ACLU) Police Tape.