Policing the Dark Web: Ethical and Legal Issues

Deliverable 4.3

University of Warwick and TNO

Co-funded by the Horizon 2020 Framework Programme of the European Union
The research leading to these results has received funding from the European Union’s Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700281.
Contents

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

1. Introduction.................................................................................1
   1.1 MEDI@4SEC.................................................................1
   1.2 Work Package 4.............................................................1
   1.3 Deliverable 4.3...............................................................1

2. Introduction to the Dark Web...................................................3
   2.1 Case-Study LEA operations on the Dark Web.........................3

3. Ethical and Legal Issues with LEA operations on the Dark Web........5
   3.1 Distinction between ethics and law......................................5
   3.2 Legal and policy discrepancies between jurisdictions...............6
   3.3 LEA engagement in harmful and/or criminal behaviour...............6
   3.4 Harms arising from the use of unusual and/or unorthodox disruption techniques.................................................................12
   3.5 Harms to law-enforcement officer welfare.............................14

4. Justifying, explaining, and weighing harms and benefits of LEA operations on the Dark Web.........................................................16
   4.1 Legitimacy and the need for a systematic, clear, and consistent approach to harms 16
   4.2 Justifying Dark Web Operations: what are the benefits?.............16

5. The role of private companies in providing LEA-facing tools and services for Dark Web investigations..................................................18
   5.1 Overview.............................................................................18
   5.2 The effect of obscure technologies on transparency, accountability and due process........................................................................19
   5.3 Tools and services using data science developed in authoritarian or human-rights violating ways.................................................................22
   5.4 Corporate Social Responsibility/Codes of Conduct for companies doing Dark Web analytics .................................................................22

6. Conclusion.................................................................................24
   6.1 Summary list of Recommendations........................................24
Executive Summary

This report discusses ethical and legal issues that arose during a workshop on Policing the Dark Web, on September 26, 2017 in The Hague, The Netherlands. The issues discussed arise in relation to LEA operations targeting illegal marketplaces and CSE (child sexual exploitation) forums on the Dark Web; and the role of private technology companies in supporting such operations.

With respect to LEA operations, which are the focus of the first half of the discussion, the report addresses the following two questions: What, if any, kinds of methods or tactics should police be prohibited from using when tackling crime on the Dark Web?’ and ‘What considerations should guide police decisions with respect to using methods that may not be prohibited, but are nevertheless seriously harmful?’ The report considers a range of relevant harms, from the re-victimisation of children, to harms to officer welfare, to interference with the exercise of freedom of expression and association online. It also considers how LEAs should approach both the task of weighing the benefits and harms of operations online and that of explaining and justifying those operations to the public.

Key recommendations emerging from this section include that LEAs should develop supplementary, detailed guidance for authorizing and covert officers doing operations on the Dark Web in order to ensure that they are carried out in ways that are necessary and proportionate; that the effectiveness of tactics and operations should be monitored systematically by LEAs over time to create the kind of evidence base on which best practices could be developed- Interpol could have an important role to play in facilitating this at an international level; LEAs should be as transparent as possible about the outcomes of operations and how these constitute effectiveness and efforts should be made to develop evaluation techniques that can measure the currently undervalued disruption effects of methods and operations.

The report then turns to a consideration of the risks and benefits that emerge from the increasingly pivotal role played by private companies in LEA operations on the Dark Web. The challenge of maintaining transparency and accountability in LEA operations given the obscurity of some of the technology and the data science it rests on is highlighted. So too is the potential impact on standards of due process for facing prosecution on the basis of evidence and intelligence gathered with the help of private companies. Finally, the potential for self-regulation of the sector via codes of conduct or corporate social responsibility initiatives is considered.

We recommend that research should be carried out to map LEA reliance on the private sector for technical tools and capabilities in investigations online, to assess LEA needs, and to forecast how this is likely to develop in the future, and that outcomes of such studies should be used to plan and invest in LEA capabilities in a strategic way. A further recommendation is that LEAs should make sure that means used by private companies they rely on are lawful and that the evidence collected is admissible in court- for example, by establishing an agreement on the way work covered by a contract will be carried out. Such an agreement could cover issues such as a commitment by private
companies to use technological methods designed to ensure the integrity of the evidence collected.

In order to ensure their relevance, the ethical and legal issues considered in this report are discussed with reference to two recent real-life LEA operations on the dark web: Operation Bayonet, which involved the takedown by LEAs of Dark Web marketplaces AlphaBay and Hansa, and Task Force Argos, an Australian anti-CSE LEA unit which involved the infiltration and running of the notorious Dark Web CSE forum ‘Child’s Play’.

The report closes by gathering together and listing the key recommendations that emerge from the discussion.
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 4.3

This document provides report identifies and discusses ethical and legal issues arising in a workshop on Policing the Dark Web, on September 26, 2017 in The Hague, The Netherlands. The workshop brought together 65 international professionals with expertise and interests in policing crime on the Dark Web. 40 of these were external delegates; the remaining 20 were from the MEDI@4SEC consortium. The group represented a diverse mix of law enforcement organisations, governments, private companies and researchers.
The workshop was hosted by TNO and took place in the framework of the international Cyber Security Week. The goal was to create an open setting to share challenges, best practices and lessons learned when policing crime facilitated by the dark web and to develop a common vision and actionable recommendations for the future policing of the Dark Web. A report on and SWOT analysis of that workshop has been produced by TNO and is available on the MEDI@4SEC Website.

This report draws on the presentations and structured discussions that took place at the MEDI@4SEC workshop to provide an initial scoping of ethical and legal issues that arise in the policing of the Dark Web. The report also reflects on how these issues might be addressed.

The issues discussed arise in relation to two broad areas of activity, namely LEA operations on the Dark Web, and the involvement of private companies in supporting the work of LEAs in Dark Web investigations.
2. Introduction to the Dark Web

The Dark Web refers to a layer of the Internet in which content has been intentionally concealed and users can surf anonymously. In order to reach the DW and to access its content, one needs to install a certain program whose function is similar to that of a web browser or search engine. The most commonly known program is The Onion Browser (TOR) (MEDI@4SEC D1.1). The feature that distinguishes the Dark Web from the open web is therefore encryption. While there is nothing ethically or legally dubious about encryption in principle, the reality is that much of the activity on the Dark Web by people in liberal democracies is unethical and/or illegal.

The Dark Web hosts a vast range of sites and forums for unethical and illegal behaviour, from illicit markets for drugs, counterfeit goods, and contract killings to money laundering, extremist sites and forums for the sharing of child sexual abuse material. All of these activities are legitimate targets of policing, and all are made easier to perform and more difficult to prevent and prosecute by encryption. However, it is not only criminals who use the dark net. Political dissidents and activists, journalists, law enforcement and the military also take advantage of the security and anonymity offered by encryption.

2.1 Case-Study LEA operations on the Dark Web

In order both to illustrate the issues raised in the following sections, and to ensure that the discussion is relevant to actual practices, we begin this section by providing a brief overview of two selected historical LEA operations on the Dark Web. These operations will serve as case-studies through which the ethical and legal issues can be explored. As such, the discussion in the remainder of the paper will refer back to these operations regularly.

2.1.1 Task Force Argos: Fighting Child Sexual Exploitation on the Dark Web

In September 2017 a Norwegian newspaper, VG, ran an exclusive report about an Australian covert police operation against a child sexual abuse forum on the Dark Web. This fascinating and ethically difficult case involved a specialist covert police unit in the Australian police force taking control of and running a CSE forum on the Dark Web for 11 months. (Other jurisdictions have also run sites, but as far as we know for a maximum of two weeks). During the time the police ran the site, thousands of images and many videos of child abuse, including live abuse, were shared on it. The officers themselves posted and shared images of child abuse.

The operation led to at least 2 very important arrests and resulted in the police taking down the site. Explaining what led them to decide to wind down the operation, police said that they stopped running it ‘when it wasn’t’ worth running …any more’.

An in-depth article about the case can be found here: https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en
2.1.2 Operation Bayonet: The takedown of Dark Web marketplaces AlphaBay and Hansa

In the summer of 2017 Europol published a press release detailing how it had supported two major law enforcement operations, (led by the US Federal Bureau of Investigation (FBI), the US Drug Enforcement Agency (DEA) Drug Enforcement Agency (DEA) and the Dutch National Police), to shut down the infrastructure of an underground criminal economy responsible for the trading of over 350 000 illicit commodities including drugs, rears and cybercrime malware. In 2016, with the help of Bitdefender, an internet security company advising Europol's European Cybercrime Centre (EC3), Europol provided Dutch authorities with an investigation lead into one of these marketplaces, called Hansa. The Dutch authorities took covert control of Hansa under Dutch judicial authority, which allowed them to monitor the activity of users without their knowledge. They also shut down a second site, AlphaBay, during the same period. This enabled them to sweep up all the new users displaced from AlphaBay who were looking for a new trading platform. According to the police’s claims, an eightfold increase in the number of new members of Hansa was recorded immediately following the shutdown of AlphaBay.

The outcomes of these combined operations were, according to the Europol press release:

- severely disrupted criminal enterprises around the world
- the arrest of key figures involved in online criminal activity
- huge amounts of intelligence (on 'high-value targets' and on the addresses of buyers) that will lead to further investigations
- seizing of millions of dollars worth of cryptocurrencies


...These two cases have led to a number of ethical and legal questions. To what extent are LEAs allowed to actively participate in or contribute to online fora containing illegal content or facilitating the selling and buying of illegal goods? And what means can be used in these situations? How to balance the means against the results that can be achieved? The issues will be discussed in the following text along the line of different types of interventions by LEAs.
3. Ethical and Legal Issues with LEA operations on the Dark Web

In this section we consider some of the ethical and legal issues arising in connection with LEA operations on the Dark Web. While each operation raises distinctive ethical and legal issues, some basic cross-cutting issues arise across all of them. Both kinds of issues are discussed below.

3.1 Distinction between ethics and law

The ethical and legal issues discussed here are distinct but related. Ethics relates to the reasons we have for thinking something is the right or wrong thing to do. Law relates to the rules a society has in place with which people can be coerced legitimately by the state into complying. Some ethical issues are reflected in the law; but ethics is broader than law: while illegal behaviour is typically also unethical, much unethical behaviour is not regulated by the law. For example, ethics tells us that breaking a promise is nearly always wrongful, even if it is sometimes justified overall given the costs of keeping the promise in the particular circumstances. Thus, ethical considerations always come into play when promise-making and promise-breaking are concerned. In contrast, legal considerations only arise when the promises in question fall within the narrower set that are legally enforceable, say in the form of contracts. Ethics is thus broader than the law, providing perspectives from which to criticize the law and argue for its reform.

To say that something is legally permissible is to say that it can be done without legal consequence. Thus legal analysis can tell us what the law requires and so what we need to do if we want to avoid being prosecuted, sued, and so on. Ethics cannot do this. But because the law usually reflects some minimum threshold of acceptability, the fact that something is lawful does not by itself demonstrate that it is desirable—let alone morally laudable or an example of best practice. Ethics can offer guidance as to what we are permitted to do, encouraged to do and required to do, morally speaking. Thus it can offer advice about what kinds of things public security providers and technology developers should do if they want their actions to be both legal and examples of best practice. Many police codes of ethics and codes of conduct include both minimum standards of behaviour and more aspirational principles. In practice, there is significant crossover between ethics and the law. For example, Privacy by Design (an approach to projects, including technology design, that promotes privacy and data protection compliance from the start) is an approach that began as best practice but is now being incorporated into EU Data Protection law. And ethics can have a key role to play in informing the law when, as is so often the case, the latter lags behind technological development.

A crossover between ethics and law also arises when both sets of principles, rules or norms share common roots. The legal issues raised in this report are grounded in and make reference to international, EU, and domestic legal instruments. The ethical issues are grounded in the values of liberal democratic political theory, including in particular

---

1 See http://ec.europa.eu/justice/data-protection/reform/index_en.htm
equal treatment, fairness, autonomy and liberty. Because the legal instruments referred to in this report are those of progressive liberal democracies, the legal and ethical concerns described below are closely related and sometimes overlap. For this reason we have presented the legal and ethical issues together in Section 3.

Sometimes the values underpinning ethics and the law conflict, and ethical and legal debates are often concerned with finding the best way to reconcile conflicting duties and obligations. Within liberal democratic societies the question of which rights, rules and requirements these values give rise to is also often subject to debate. Finally, the interpretation of the role and status of the police and the nature and source of their authority varies significantly between liberal democratic countries. As this suggests, shared roots and basic commitments do not preclude dilemmas and disagreements within both ethics and the law.

3.2 Legal and policy discrepancies between jurisdictions

Divergence between LEA law and practice in different countries illustrates a lack of consensus about how much weight should be given to the harms of each of those kinds of behaviours when assessing the proportionality of LEA methods. For example, in Australia police are prohibited from physically abusing children but permitted by law to share images of child abuse online. In a so-called ‘controlled operation’ they get specific permission from a judge to do so. In many other jurisdictions, such sharing is illegal. In some jurisdictions, LEAs may be permitted to set up sites for the sale of illicit material on the Dark Web. In others they may only be allowed to take over and host such sites when they have been created by others.

The length of time for which LEAs are permitted to host such sites also appears to differ between jurisdictions, again reflecting differences in assessments of the harm caused by facilitation of crime. For example, while Australian police have hosted CSE sites for 6 and 11 months respectively, the maximum time the FBI has hosted an illegal marketplace was 2 weeks.

There is a risk that LEA cooperation is used as a means to transfer operations to the auspices of LEAs in jurisdictions that are more permissive when it comes to the tactics and timescales of such operations. Greater harmonization between jurisdictions and LEAs operating practices is desirable so as to retain democratic accountability and legitimacy. Europol and Interpol could have a key role to play in facilitating such harmonization.

3.3 LEA engagement in harmful and/or criminal behaviour

Both of the Dark Web LEA operations outlined above involve police engaging in activity that would be considered serious criminality if undertaken by a regular citizen. Dark Web operations are by no means the only contexts in which LEAs may end up deciding

---

2 Seminal philosophers in this field include: John Locke; Immanuel Kant; John Rawls; Ronald Dworkin; J.S. Mill.
to act in ways that would otherwise be considered serious crimes. But success in Dark Web operations seems almost inevitably to rest on LEA willingness to engage in such activity, be it dealing drugs or weapons, money laundering, hacking, or sharing images of child sexual abuse. LEAs are therefore likely to face dilemmas around the use of otherwise criminal and often very harmful methods with increasing frequency, as illegal activity on the Dark Web continues to grow apace.

Engaging in criminal activities by LEAs is not always legally permitted. Going undercover to infiltrate in a network of criminals is a common method to gain knowledge about the criminals in order to arrest them. But this might involve participating in criminal activities as well. What is allowed and what is not allowed depends on the situations an agent gets involved in and always requires a legal and ethical consideration. In the Netherlands, infiltration is allowed, but entrapment is not. In case an action is a form of entrapment, the result is that an illegal action takes place by a citizen, which would not have occurred if the police did not set the trap. Legally, this implies that there was no intent of the citizen to commit the crime, so in case of a court case the sentence will be lower or absent. Clearly, the boundaries between engagement and entrapment get blurred to a certain extent. The distinction as explained during the workshop lies between maintaining a marketplace and actively creating a new marketplace by a LEA. Nevertheless, even maintenance requires action and includes facilitating the offering of illegal goods or content. Creating a marketplace with illegal would seem a form of entrapment, including the legal implications mentioned above. Moreover, the type of goods may bring a difference. Offering drugs or weapons without delivering them can be allowed, while offering child abuse images may not be, since the offering may include providing or spreading the images instantly. Basically, providing or spreading images of child sexual abuse is illegal as such.

LEAs considering using otherwise criminal tactics are constrained in doing so by both moral and legal principles. Not only do they need to demonstrate that the harm they cause is proportionate to the harms prevented, but they must also have regard to moral and legal prohibitions on the use of certain methods. Two questions therefore arise: ‘What, if any, kinds of methods or tactics should police be prohibited from using when tackling crime on the Dark Web?’ and ‘What considerations should guide police decisions with respect to using methods that may not be prohibited, but are nevertheless seriously harmful?’ We now discuss these two questions in detail.

3.3.1 Prohibited methods—entrapment and violations of fundamental human rights

There are certain methods police are legally prohibited from using, whatever the potential benefits to criminal justice. Two categories of prohibited methods are relevant here.

---

4 See the Tallon case from the Dutch Supreme Court (Hoge Raad): Tallon-arrest, HR 4 december 1979, NJ 1980, 356.

Entrapment

The first is entrapment. The moral prohibition on entrapment is essentially a prohibition on giving someone an exceptional or unique opportunity to commit a crime and thereby having an essential role in turning them into a criminal. The rationale for such a prohibition is that the role of police in a liberal democracy is to prevent crime—not to provide people with the temptation to commit it. Moreover, for the legal qualification of a criminal act, intent is often a requirement. If a situation is created where the opportunity to commit a crime is presented in such a way that it is more difficult for the criminal to step aside than to continue, the intention might be less rational and therewith difficult to prove in court. Under the ECHR, the Court’s approach to whether entrapment was at stake or not is currently of an objective nature. The Court holds it irrelevant whether the target had had a latent criminal intent (whether he had been predisposed) before the agents’ intervention; the relevant element was whether he had started acting upon his latent criminal intent before the intervention. There is thus no difference for entrapment purposes between the creation of a criminal intent that had previously been absent and the exposure of a latent pre-existing criminal intent.6

Until now, Dark Web operations running illicit marketplaces and forums have not crossed the line into entrapment because they have only involved the continuation of existing sites, not the creation of new or unique ones. This is likely what Jon Rouse, Detective Inspector on the Child’s Play operation intended when he insisted that his unit ‘will never create a forum for child sex offenders’.

The distinction between creating and maintaining a website on which serious criminal activity takes place can be compared to offline situations. For example, it is known practice for police who become aware of an impending drugs deal to go undercover and pretend to be the dealer or buyer in order to arrest someone. The offer and the deal are not created, but rather maintained and then interrupted by the police. Nevertheless, the line appears thinner in the case of maintaining a platform for child sexual content or other types of illicit digital content, when doing so means the illegal material is in fact shared or delivered. This contrasts with the example of a drugs deal, where the drugs itself is not actually ever delivered to a genuine buyer. Maintaining platforms with instantly available digital content of an illegal nature implies that the illegal products are not only delivered but received as well.

Even when LEA operations on the Dark Web use methods that fall short of entrapment, these may still raise important and related ethical issues such as the facilitation or encouragement of crime. These are discussed in more detail below.

Violations of fundamental human rights

In most liberal democracies, there are certain things police are not permitted to do, whatever the harm they are trying to prevent. These prohibited methods include torture, rape, child abuse, and assassinations. One of the moral reasons for prohibiting

---

such actions is that the act of carrying them out compromises the moral character of the actor in question. In other words, even if one only carries out torture in order to save many lives, in doing so one still becomes a torturer. When it comes to actions carried out by LEAs, it is not just the moral character of the individual police officer that is in question; it is also the moral character of the entire political community, because in a democracy police officers act in the name of and with the political authorization of the public. Some might argue that a democratic state cannot continue to claim legitimately to be founded on respect for the dignity and equality of human beings if it compromises its moral integrity with acts that violate such principles.

3.3.2 Potentially permissible but controversial methods: necessity and proportionality
But while there is a consensus around the moral and legal prohibition on committing certain kinds of harms, like selling dangerous drugs or weapons, or abusing a child, there is legal and moral divergence on the issue of whether police should facilitate or encourage such harms, or even just to stand by and allow them to occur when intervention might have been possible.

Both morality and the law generally reflect our moral intuitions that there is a descending scale which states roughly that directly inflicting a particular harm is worse than facilitating it, which in turn is worse than encouraging it, which is worse, in turn, than merely allowing it to occur when one had an opportunity to intervene to stop it.

When police run Dark Web forums such as Hansa or Child’s Play, they engage in all of these kinds of wrongs or harms. For example, going undercover as a paedophile might involve behaviour that directly harms children by sharing images of their abuse with paedophiles; encourages abuse by egging others on in their sharing of images; normalizes abuse by befriending other paedophiles and making them feel comfortable about their acts; and permits abuse to happen by standing by and witnessing it—live online in some cases—instead of intervening to prevent it. These aspects of covert policing are often overlooked in public discussion and scholarly analysis, both of which focus on the potential impact of law-enforcement activity on those individuals who are rightly or wrongly suspected of crime.

In strictly legal terms, such LEA activity may directly infringe upon the human right to bodily integrity (respect for the human body). Even screenshots or previews in thumbnails may qualify as such under the law.

When it comes to justifying the use of such methods, LEAs in all EU countries rely on a framework based on the moral and legal principles of necessity and proportionality. These principles state, roughly speaking, that LEAs should use the least harmful and intrusive means necessary to achieve their criminal justice aims, and that any harms and intrusions thus caused should be proportionate to those aims.

In the remainder of this section, we provide some indication of the kind of harms that might occur in the context of Dark Web operations and how LEAs might begin to incorporate them into proportionality and necessity assessments as well as into guidance and future planning.
3.3.3 Doing harm: re-victimising vulnerable people and/or using them as a means to the pursuit of criminal justice ends

Some methods used by LEAs in operations on the Dark Web involve the re-victimisation of people who have been the victims of crime. This related in particular to police sharing of images of abuse, be it child abuse, torture by terrorists, or some other kind of abuse. Sharing of such images and videos involves violating someone’s basic rights and interests, not for their own protection, but for the sake of some other criminal justice aim. In other words, they involve using someone as a means to an end, rather than respecting them as an individual with basic rights that should never be violated. This is perhaps what one mother – interviewed for the Norwegian newspaper report on the Child’s Play operation – meant when she said she felt that police posing as paedophiles used her daughter ‘as bait’ with which to catch criminals when they shared images of her abuse with other paedophiles while undercover.

One potential line of justification for such re-victimisation might claim that the sharing of images of abuse may be permissible provided that it is minimized, and that it is justified in terms of protecting other, similarly vulnerable individuals, from the same kinds of abuses in the future. This is likely what Jon Rouse, a Det. Inspector with Taskforce Argos meant when he insisted that Argos is a ‘victim-centred unit not an offender-centred unit’. According to this viewpoint, the fact that the wrong done to the individual is done precisely to protect others like them makes it less damaging to the dignity of the victim, and therefore less difficult to justify than it would be if it were done merely to catch criminals.

If LEAs considering using this tactic are to rely on this justification for re-victimising abused children, then they should ensure that the aim of the operation is explicitly defined in terms of the protection of victims and that its success is measured with reference primarily to victim protection rather than arrests. (Often the latter will track the former, but it may not always do so, for example if one member of a child sexual exploitation gang is arrested this may not reduce the exploitation of the children targeted by that gang significantly). They should also spell out in guidance to officers the conditions under which such actions are permissible, to ensure that re-victimisation is properly limited. And they should develop a policy on consulting and/or compensating victims whose images are shared and, where appropriate, their families. As lawyer James Marsh stated in relation to the Child’s Play operation: ‘If victims could be consulted along the way, it would give them a sense of control. Control is exactly what they were deprived of during the assaults’.

From a legal perspective, re-victimisation as a means to protect other (potential) victims implies that a rather explicit choice has to be made to prioritize prevention and protection above catching criminals. However, catching criminals and stopping criminal activity will usually be the trigger to engage in re-victimisation. With regards to proportionality and necessity, therefore, a proper assessment will always be needed, including continuously monitoring and assessing the actions of LEAs along the way. The difficulty is that it may be hard to decide to halt or roll back on activities involving re-

---

1 Speaking in a video on YouTube [https://www.youtube.com/watch?v=5CJKeQnnoW8](https://www.youtube.com/watch?v=5CJKeQnnoW8).
victimisation if there appears to be is an increasing chance to catch one or more criminals behind a network. Guidelines and standards for performing these kinds of assessments could be a very valuable and helpful tool for LEAs in these complex situations. The guidelines may include basic principles and guidance on how to weigh interests and how to make legal and ethical considerations in specific cases.

3.3.4 Encouraging, facilitating, and normalizing harm

While there exists a well-developed body of domestic law on entrapment in most jurisdictions, legal and moral norms are less clear when it comes to activities that are related to, but fall short of entrapment, like encouraging or facilitating crime. Running Hansa and Child’s Play sites, as LEAs did in our two case-study operations, involved the facilitation of crime, because the sites were designed and established with a purpose of enabling people to exchange illicit materials. While the police takeover of these sites did not create new opportunities to commit crimes, it did enable those intent on committing crimes to do so. As a result, some criminality occurred on the LEA’s watch, which would not have occurred if they had simply closed down the site. This kind of facilitation of crime can be justified by the aims of the operation, which might reasonably be more ambitious than merely taking down a site—as that would most likely merely delay such criminality until it can find a new site to which to migrate.

Encouraging crime is more likely to occur when operations entail officers going undercover and adopting identities in ways that involve making friendships or collaborating with criminals. This is probably more typical of counter-terrorism or anti-paedophile operations than with operations to disrupt dark markets such as Hansa. For example, the Child’s Play operation involved officers making ‘friends’ with other paedophiles, expressing approval of and ‘liking’ images or videos of abuse, and potentially encouraging them to continue to post images. When asked how his unit justified these activities, Jon Rouse, one of the leading officers in Taskforce Argos, replied that ‘abusers are abusers’ and that ‘people who have a desire to abuse children will abuse children no matter what’. This response seems to indicate an assertion that police actions cannot turn someone into an offender who was not already going to become one. But while this might be true when applied to the impact of actions taken by an individual undercover officer, it is probably also true that some paedophiles would not have become contact offenders were it not for the existence of sites such as Child’s Play, where abuse is normalized and encouraged. When LEA activity contributes to this cumulative kind of encouragement, this should be acknowledged and taken into account in any assessment of the harms caused by those tactics.

3.3.5 Allowing harm

Similar points can be made in relation to the fact that LEA operations on the Dark Web often involve police having direct knowledge and/or witnessing the occurrence of serious crimes but not taking opportunities to intervene to prevent them. Here again a range of relevant considerations come into play and these should be worked into a coherent approach to weighing the harm of such omissions. Such considerations include, for example, the seriousness of the crime; its imminence; the reliability of the intelligence or evidence of its occurrence; the likelihood of success of any policy
intervention to stop it; and the potential effect of such intervention on the broader aims of the operation.

Generally speaking, allowing harm to occur is not as objectionable morally as either directly inflicting it, or encouraging or facilitating it. Nevertheless, it is important to clarify a policy with respect to allowing harm, because the stakes can be very high. For example, in the Child’s Play operation, police officers witnessed child abuse occurring live online and did not act to prevent it. One can speculate that they also allowed dangerous drugs and even lethal weapons to be traded on Hansa while they were running the site. People may well have died as a result of the trade of such things. Allowing such harms might be justifiable if the alternative of direct intervention would serve only to displace the specific incident and would likely risk undermining the larger operation. But it is not clear whether the LEAs involved in the two operations outlined above attempted either to predict or to retrospectively assess the harm caused by these criminal acts, or both. Such assessments are important both for those making decisions about whether to extend authorisations for certain covert activities and for future strategy and planning, which should be informed by evidence and knowledge gathered from historical operations.

There is a risk that LEAs carrying out long-term, high-stakes operations become so invested in the operation that they are willing to allow very serious and very harmful crimes to occur if that appears necessary to the success of the operation. For example, in the Child’s Play case, the police were following and watching the two key administrators of the site for 3 days before they arrested them. During this time, the criminals met in person, checked into a hotel, then went together to a house where they raped a 4 year-old child. The police were watching the house when the abuse occurred. It is unclear from what the police have said why did they not intervene to arrest these individuals before they visited the house. It is also unclear if (and if so then why) they did not check whether a child was living at the address they visited or whether the person registered to that address had access to children. The criminals were eventually prosecuted for the rape of that 4-year old rather than for their role in administering the Dark Web site. This raises the question whether the LEAs decided not to intervene earlier but to take the risk that their targets would abuse a child, in order to help secure a prosecution, and whether doing so is ever justified. Such questions cannot be addressed unless LEAs are clearer with the public about the way in which they make decisions.

3.4 Harms arising from the use of unusual and/or unorthodox disruption techniques

Certain features of the Dark Web, in particular the difficulty of tracing activities back to identifiable people and locations, and the internationally distributed nature of criminal activity, make it difficult to apply traditional LEA approaches. As a result, activities designed to disrupt illicit activity by taking advantage of anonymity and the fragile basis of trust on the Dark Web have become more attractive to LEAs. These might include:
• spreading misinformation, fake news, and rumour to fuel mistaken beliefs about police activities online and to reduce trust between e.g. buyers and sellers of illicit products.
• using technological means, such as DDS techniques which overwhelm outlets and force them to close, in order to disrupt the supply chain online
• using ‘honey pot’ techniques, such as using automatic tools to pretend to be vendors and “sell” drugs, so that users get scammed and don’t return to the market.
• advertising LEA’s own successes to show that they operate confidently on the Dark Web, which would reduce trust in encryption. For example, the Dutch national police have created a dark web site that lists Dark Web vendors by pseudonym, including those under investigation, those who are “identified,” and who have already been arrested in current and past investigations. "We trace people who are active at Dark Markets and offer illicit goods or services," the site reads. "Are you one of them? Then you have our attention."

Such tactics might be effective in deterring crime on the Dark Web, however they may also have negative implications, which are now considered below.

3.4.1 The risk of criminalizing innocuous behaviour and/or undermining the exercise of valuable freedoms facilitated by the Dark Web

Not all activity on the Dark Web is suspect. Some citizens use the Dark Web as they do the open web. For example, ethnographic research on one particular Dark Web site- the Dark Web Social Network- in 2014, describes a politically libertarian but innocuous website, used by people who see it as a means of being free from the kind of corporate and government surveillance they find objectionable on the open web. As that research reports, the Dark Web Social Network’s ‘about’ page describes it as “a safe and moderated environment for the productive exchange of information.” Notably, that research also found that the Dark Web Social Network discouraged child sexual exploitation images and policed itself relatively successfully. Similar processes of moral policing on the Dark Web were also reported in more recent research based on interviews with administrators of Dark Web search engines. And tech commentators and researchers routinely predict that more and more everyday and innocuous ‘surface web’ activity will migrate to the Dark Web as people become more concerned about their privacy and less tolerant of corporate monitoring of their behaviour for marketing purposes. Privacy and censorship concerns also are emerging as significant predictors.

---

11 Bartlett, Jamie, ‘Hoe the mysterious dark bet is going mainstream’ TED talk, available at: https://www.ted.com/talks/jamie_bartlett_hoe_the_mysterious_dark_bet_is_going_mainstream
of reduced opposition to the Dark Web,\textsuperscript{12} as a reported surge of Dark Web usage following the Edward Snowden revelations appears to confirm.\textsuperscript{13}

For many using the Dark Web, their activities are not only innocuous but also constitute the exercise of valuable freedoms. Chief amongst these are the freedom to express political views or sexual preferences without fear of persecution by authoritarian regimes and the freedom to exchange information without manipulation or monitoring by profit-seeking companies. Some Dark Web users consider the term ‘dark net’ or ‘Dark Web’ itself a media fabrication to draw attention away from the legitimate, innocuous, and even life-saving use of the Dark Web and towards the criminal. Some, like Edward Snowden and Julian Assange, see government-sponsored attempts to crack anonymity on the Dark Web as an attack on freedoms, especially privacy.\textsuperscript{14}

An LEA approach to the Dark Web that treated all activity there as suspect in an undifferentiated, blanket manner would risk undermining the exercise of these freedoms. For example, attempting to crack encryption and expose the identities of individuals interacting anonymously on the Dark Web might not only expose those particular individuals to harms from authoritarian governments, but also undermine the trust that is vital to the effective function of the Dark Web as a space safe from political persecution. For this reason, \textbf{LEAs in liberal democratic jurisdictions should as far as possible adopt a targeted approach to policing the Dark Web, focusing on exposing, disrupting and prosecuting criminals while refraining from interfering with innocuous activities and the exercise of political freedoms.}

\subsection*{3.5 Harms to law-enforcement officer welfare}

Until now we have focused on the harms of LEA Dark Web operations on victims. But such operations also have a high cost for the individual officers carrying them out. At the beginning of this Section we noted that certain methods are out of bounds in liberal democracies, partly because of the impact on the moral character of those carrying them out. Reports of covert operations on the Dark Web certainly demonstrate that the individual officers involved struggle to maintain their moral identity, if not their moral compass. This is illustrated by the words of one Australian officer who went undercover as the person running an online child sexual abuse forum: ‘It’s as if you force yourself to have a split personality, and you download this other person into a part of your brain and hand over that part of your brain to him. It’s hard. \textit{You give a part of yourself the job, and that part becomes a friend of those you’re investigating. When we were done with one of our recent operations, it felt like I had locked up all my friends}.’ This describes a professional hazard that has serious implications for the welfare of covert officers, towards whom LEAs have a duty of care. But it is also an issue of preserving valuable expertise and skills within LEAs: officers who have breakdowns or who can no longer perceive the distinction between morally acceptable and

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{12} Jardine Eric. (2017) ‘Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies’. \textit{New Media and Society}. Online First. October 4, 2017
\item \textsuperscript{13} Gehl, 2016a (as above).
\end{itemize}
\end{footnotesize}
unacceptable tactics can become a risk rather than an asset to covert units. **LEAs should** put in place strategic and long-term provision of psychological, moral, and professional support for officers involved in operations that bring them close to disturbing activities such as torture and child abuse.
4. Justifying, explaining, and weighing harms and benefits of LEA operations on the Dark Web

The previous section discussed the kind of harms that are inflicted by or occur in the context of LEA operations on the Dark Web. This section focuses on the approach LEAs can and should take to weighing, explaining, and justifying such harms, given the aims of policing and the legal limits on police action.

4.1 Legitimacy and the need for a systematic, clear, and consistent approach to harms

Only by developing a systematic, clear and consistent approach to navigating the harms of Dark Web policing methods can LEAs begin to respond to the inevitably increasing rounds of criticism their operations receive. For an example of such criticism, we can consider the following quote from Carissa Byrne Hessick, a professor of law and legal expert in this field, who reacted to reports of the Australian police’s hosting and takedown of Child’s Play thus:

“It sounds like the police tell one story about how damaging the images are when others share them, and another story when the police share them. That’s a kind of hypocrisy I really don’t like. But this sheds light on the argument that any and all sharing of such an image is abuse. If the police say they’re only sharing images that have been shared before, it means the police do not think all sharing is harmful.”

This criticism is unfair. It assumes wrongly that LEAs have no ground for arguing that there is a moral (and that there should be a legal) difference between the harm of sharing of images for a limited time in order to protect other victims and the sharing of images in order to achieve access to other images, satisfy abusive urges, and fuel further abuse. But doing harm in order to avert further, more serious harm is in principle justifiable whereas doing harm in order to satisfy one’s desires is not. LEA clarity around the use of controversial methods is essential if the inevitably difficult operations in this area are to retain legitimacy and public support.

4.2 Justifying Dark Web Operations: what are the benefits?

As the previous paragraph suggests, public acceptance of LEA methods in Dark Web operations depends on such methods being clearly and consistently justified by the LEAs using them. This includes spelling out the benefits that such tactics are deployed to achieve. But sometimes those benefits are poorly defined. A review of official and journalistic reports of the Dark Web operations described above reveals that they are justified in terms of: victims identified; arrests and convictions; and abusers ‘identified’. While these are all legitimate aims of law enforcement operations, they leave out crimes averted or disrupted, and deterrence. These should be included amongst the outcomes.

---

15 VG article
by which success is measured. In other words, efforts should be made to develop evaluation techniques that can measure the value of deterrence and disruption.

More importantly, the positive outcomes of Dark Web operations are described by police in very broad and general terms. It is desirable that the outcomes are measurable and able to be monitored, not only so that the benefits of the operation can be properly understood and then balanced against the harms, but also so that a body of evidence about the value of these operations and the tactics used during them can be amassed. This means, amongst other things, creating measurements that are finer-grained than simply numbers of individuals arrested. For example, an operation that results in the conviction of 5 small-time drug dealers is less successful than one which results in the conviction of a single, very serious and prolific repeat offender. Counting the severity of the sentences, e.g. number of years of imprisonment, would better track the harms averted.

LEAs should think carefully and systematically about the nature of and the weight that should be given to the harms of the different kinds of methods they use when undertaking operations on the Dark Web, and how they can be justified. **LEAs should develop guidance for authorizing and covert officers doing operations on the Dark Web in order to ensure that they are carried out in ways that are compatible with respect for human rights and with the ethical codes that govern policing in many jurisdictions.** The effectiveness of tactics and operations should be monitored over time to create the kind of evidence base on which best practices could be developed. In this respect, it would be desirable to form an international evidence-base and bank of tactics in order to enable the diffusion of best practices amongst forces across jurisdictions. Interpol could have an important role to play in any such initiative, and indeed it appears that they have already begun to be proactive in this area, developing INTERPOL investment in technologies for cybercrime. However, as the following section explains, much of the technology used by LEAs to support their operations on the Dark Web are provided by private companies, and this raises a set of distinct ethical and legal issues, to which we now turn.
5. The role of private companies in providing LEA-facing tools and services for Dark Web investigations

5.1 Overview

Private companies are playing an increasingly pivotal role in LEA operations on the Dark Web. For example, the investigation lead which enabled Dutch authorities to target the Hansa marketplace was identified with the help of Bitdefender, an internet security company advising Europol’s European Cybercrime Centre (EC3). Private tech companies have the data, expertise, and tools to support investigations to achieve outcomes that would be beyond the capabilities of LEAs working alone. They are making a significant contribution to law enforcement on the Dark Web. While this contribution is certainly welcome, there is a risk that it is accompanied by an increasing hoarding of capabilities within the private sector, creating a risk that LEAs become overly reliant on the services of companies in ways that have implications for accountability, transparency, the right to a fair trial and taxpayer value for money.

One way in which these risks may arise is if certain companies become indispensable to LEA work through the construction of databases that cannot be replicated by LEAs. For example, one company that presented at the MEDI@4SEC workshop on the Dark Web reported that it had amassed and stored Bitcoin metadata over a period of years. This company therefore has a de facto monopoly on the market for this data, which is increasingly useful as it can reveal information that can help to expose the identities of individuals or to track accounts on the Dark Web.

Anecdotally, participants in the MEDI@4SEC workshop on the Dark Web expressed concern that companies are charging huge sums for information that would be very useful to police investigations, making investigations unduly expensive. The concern was also expressed that LEAs find it very difficult to recruit people from these companies, because they cannot compete in terms of attractive salary packages. In addition, it was noted that LEA procurement procedures are long and burdensome, making it difficult for LEAs to respond in a timely manner to operational challenges. Finally, the concern was expressed that LEAs may make poor procurement decisions, buying tools that are very expensive but which may become obsolete quite quickly, given how fast technology develops in this field.

At the same time, it was reported that opportunities exist for LEAs to get external technical expertise and assistance without high costs. For example, a small number of private entities provide information to LEAs for free, or work with them on a pro bono basis. In addition, the role of the VG newspaper in identifying the Child’s Play server shows further that tech-savvy investigative journalism could play an important role in assisting police. Digilante or white hat hacker groups could also be engaged by LEAs to assist in operations that target common enemies, such as child sex offenders on the Dark Web. For instance, in 2014 Intangir, the pseudonym for a hacker who acts as a self-styled patrolman of the Dark Web, deleted all the child sexual abuse-related links from a
popular site called Hidden Wiki.\(^{16}\) Or they could provide useful insight into techniques useful to investigators- for example, citizen journalist group Bellingcat provide an open source tutorial on their website on how to do investigations on Bitcoin transactions.\(^{17}\)

Yet even if these alternative routes to gaining valuable expertise, skills, and tools are likely to be fruitful, they are unlikely to significantly reduce the reliance by LEAs on private companies. This is a problem not only because it may drive up the costs of LEA operations on the Dark Web, but also because private companies act out of self-interest in an area of activity that has an impact on the public interest, as we now discuss in more detail.\(^{18}\) Our observations below support the conclusion that research should be carried out to map LEA reliance on the private sector for technical tools and capabilities in investigations online, to assess LEA needs, and to forecast how this is likely to develop in the future. The outcomes of such studies should be used to invest in LEA capabilities in a strategic way.

### 5.2 The effect of obscure technologies on transparency, accountability and due process

#### 5.2.1 Transparency and accountability

Transparency and accountability of LEA activity is vital for its democratic authorization, both directly by formal mechanisms of oversight, and indirectly by the public. Secrecy around technological methods used to support such operations raises the question of whether and how elected officials, national audit bodies, police oversight agencies, and journalists will be able to scrutinize the work of LEAs to ensure that criminal justice decisions are being made fairly. And techniques and algorithms used by private companies may well kept secret. This raises potential challenges for transparency and accountability of LEA operations that rely on such techniques. This is a real problem, not only a hypothetical one: at the time of writing journalists in the USA are pursuing litigation against the Chicago Police Dept. to force it to reveal algorithms it uses to determine who is high-risk enough to be placed on a predictive policing gun violence ‘heat list’.\(^{19}\) The need for such revelation was given further impetus by a 2016 study by the Rand Corporation, which found that being on the heat list was not in fact predictive of future involvement in gun crime, as the Chicago Police Dept. claimed it was.\(^{20}\) This problem is likely to become more relevant in the future as cooperation with private companies becomes increasingly necessary for LEAs to be able to properly investigate criminal activity on the Dark Web.

---

\(^{16}\) See the report here: https://motherboard.vice.com/en_us/article/539ggq/a-hacker-scrubbed-child-porn-links-from-the-dark-webs-most-popular-site

\(^{17}\) https://www.bellingcat.com/resources/2017/09/15/follow-bitcoin-python-blockexplorer-webhose-io/

\(^{18}\) For an excellent in-depth analysis of some of these issues, see Joh, Elizabeth (2017) ‘The Undue influence of surveillance technology companies on policing’. New York University Law Review, 92.


A second way in which the involvement of private companies in supporting LEA operations on the Dark Web might undermine transparency and accountability is by using complex and obscure algorithms. Understanding the workings of the algorithms may be difficult for LEAs. But if the basis on which LEA resources are allocated and criminal justice decisions are made is obscure, then it is difficult for LEAs themselves to be sure that they act fairly and in the public interest, and it is even harder for relevant external bodies and institutions to exercise effective democratic oversight. This issue arises not only when resources of private companies are used upfront to indicate target groups, but also when there is cooperation between LEAs and private companies during an operation.

5.2.2 Due process

After investigations have taken place by LEAs in cooperation with private companies, criminals have to be taken to court. In these cases, it is required both that the evidence collected and that the way the evidence has been collected become transparent. In light of due process and the right to a fair trial in which a suspect can properly defend himself, there can be no secrets regarding the evidence. Moreover, the evidence needs to have been obtained lawfully. Unlawfully obtained evidence needs to be excluded from the trial and cannot be allowed to count as evidence to come to a conviction. Due process issues arise when technology used to gather evidence is not made transparent and when it is made transparent to the relevant legal parties but is too technically complex for them to understand and evaluate sufficiently well.

The admissibility in court of digital evidence has been a subject of debate for some time. The difficulty judges face in understanding digital evidence is a problem. So too is the need to prove that evidence is ‘real’ and has not been digitally manipulated. These issues are precisely what can make it difficult to consider the evidence as ‘convincing for a judge’. The essence of a law trial is that the judge has to be convinced of the fact that a suspect has committed a crime in order to come to a conviction. The judge weighs all the relevant evidence at hand and then comes to a decision of whether he or she considers the evidence to be convincing. Difficulties in weighing the evidence arise in relation to Dark Web activities in particular, because of the technical complexities.

In collaborations with private companies opportunities may arise to obtain more or other types of evidence than LEAs could be allowed by law to collect on their own or to perform certain actions or activities that may not be performed by LEAs. In this situation, cooperation with private companies can be used as a means to extend the methods available for LEAs during their investigations, potentially beyond the legal limitations or competences that apply to LEAs. Legal boundaries on competences should be kept in mind carefully.

However, with regards to admissibility of evidence some legal guidance is available. The case law of the ECHR acknowledges that the national legislator is better placed to deal with the (substantive) law of evidence. So national differences can arise. However, it is possible to find some clarity with respect to the requirements for procedural fairness of
The case of Khan v. UK\textsuperscript{21} may be invoked as a leading case in this matter. In this case, the police had installed listening devices in the private property of Khan, without his knowledge. The tapes recorded were obtained in breach of article 8 ECHR (right to private and family life), but the court had taken considerable account of this unlawfulness and the lack of regulations providing Khan with remedies. A breach of article 8 was upheld, but the evidence was admissible, since the court had properly considered all evidence and taken account of the unlawfulness of the recordings as part of the evidence. It follows from this decision that the provisions of article 6 ECHR, the requirement of a fair trial, concern criminal proceedings in their entirety and cannot be limited to a single item of evidence. So, if a piece of evidence has been obtained by using unlawful means, this does not automatically undermine due process, providing a defendant is given the opportunity to question the significance and legality of the evidence and its source, and whether it was falsified before a court.\textsuperscript{22} The legality of evidence may depend on the extent to which a LEA has had a hand in instructing a private party to obtain the evidence if this happened in an unlawful manner. If a LEA knows that obtaining evidence in a certain way is unlawful but nevertheless instructs a private party to obtain the evidence in this way, the evidence will be unlawfully obtained and can be excluded from the trial. However, if a private party collects evidence on its own initiative, which can be in an unlawful manner, and delivers the evidence to a LEA, the evidence may be lawfully obtained by the LEA and can as such be included in the trial.

In addition to the problem of determining whether evidence is admissible, there is also a potential challenge around guaranteeing the transparency of the process of the trial. So, all evidence that is used to come to a judgement needs to be available to all parties. This does not necessarily include the methods for obtaining the evidence. However, when it concerns digital evidence about behaviour of a suspect on the Dark Web, the methods of obtaining evidence may be implicitly part of the evidence itself. To see how this is the case, it’s useful to consider the use of algorithms to identify suspects. Technologies relying on algorithms can be used to give guidance to LEAs on where to search for suspects or illegal activity. However, this profiling technology cannot be evidence in itself, as it only indicates potential suspects. It can be the starting point for investigations, but still then the illegal activity needs to be identified, recorded, and proven in relation to a suspect before a conviction can take place. In any case, when there are indications based on profiling that a specific activity or person should be investigated, the LEA has to be able to explain to a judge why the indication was indeed sufficient to start using means for investigation. The reason is that the use of specific investigatory means needs to be justified. Otherwise, the investigations can be declared to be based on arbitrariness.

In practice, LEAs may be provided with intelligence by private companies, but LEAs do not disclose this in court because doing so would jeopardize the relationship with the

\textsuperscript{21} 12 May 2000 (Application No 35394/97).
\textsuperscript{22} A. Roosendaal & N. Purtova (2009). Whether a Photograph Taken for Google’s Street View can be used as Evidence in a Criminal Process: A Case Note. Digital Evidence and Electronic Signature Law Review, vol 6, p. 187-190.
company. This illustrates that there is a certain kind of dependence of LEAs on private companies, since these companies might have better means and knowledge to gather specific intelligence. However, keeping this a secret in court might infringe upon the right to a fair trial if a suspect is not able to assess the origins of evidence. There is a risk of LEAs trying to hide their collaborations with private companies, which might imply that there is a need to ‘build a story’ of the evidence and how it was obtained and why a certain investigation was started. All this, to defend proactively against arbitrariness.

5.3 Tools and services using data science developed in authoritarian or human-rights violating ways

As indicated, LEAs are bound by law to use only certain permitted means to pursue an investigation. The use or application of data science technologies is permissible as long as these fall within the scope of means and competences allowed, often by national laws. The question arises whether EU LEAs should be buying or contracting to use such services if the science behind them has been developed by using data in ways that would be illegal in EU jurisdictions. A clear answer to this question is difficult to give. First, it may be difficult to an LEA to know about the exact way a service has been developed. Basically, the services do not come with a description of the exact means of development and the exact technologies or databases used to build a certain standard of techniques, knowledge, or profiles. Second, it may be possible to find out about the way a service has been developed, but this does not automatically also provide information about whether the way it is applied in practice or works in its deployment is legal or not.

In any case, LEAs can only use the services provided by private parties in ways that are in line with their legal competences. Some means fall outside the legal competences of LEAs. For instance, if a private company is hacking a computer or a network by using illegal hacking software, this is a way of obtaining evidence or at least gaining access to a network that falls outside the scope of the legal competences of LEAs.

5.4 Corporate Social Responsibility/Codes of Conduct for companies doing Dark Web analytics

In order to give some more guidance on private companies offering services for Dark Web analytics or research, the development of a Code of Conduct may be desirable. Given the fact that there is a strong focus on illegal activities and finding or obstructing these, clear rules or a set of basic principles can be helpful in creating an accountable practice. The sharing of best practices can be useful as well.

With regard to the principles, inspiration can be found in several human rights laws. For instance, the requirements for due process as discussed above can give some guidance on transparency that is needed for legal admissibility of evidence or investigation techniques and technologies. A parallel can be drawn with the basic principles for information security, often referred to as the CIA-principles. CIA stands for Confidentiality, Integrity, and Availability. So, information collected in the course of investigations should be protected properly against leakage or unlawful access, the integrity of the data needs to be ensured, e.g. by using time stamps of digital signatures,
and the data need to be kept available and should not be lost or get out of sight. Besides, laws on privacy and data protection can be used to formulate principles. For instance, the principle of privacy by design (or data protection by design as laid down in Article 25 of the GDPR) can be used as a way to protect the rights of individuals that behave lawfully on the Dark Web. The principle entails that in the development of tools or services, the protection of privacy is embedded. This can be done by implementing techniques to secure the data, by anonymizing or pseudonymizing the data when possible, and by means of contracts and working instructions. In general, the measures taken can be of a technical or organizational nature. The aim of privacy by design is to protect the fundamental rights of persons whose data is being processed. These persons can be suspects, but also other persons whose data is being processed in the course of investigations, simply because more data is collected than from the suspect only. The application of privacy by design seems a logical step, since the reason for using the Dark Web for non-criminal activities can often be found in privacy considerations of individual users. But privacy by design can also help to protect the rights of suspects, because it supports the creation of requirements on how to secure data and how to ensure integrity of the data collected. Data integrity and quality of data are aspects that should be taken account for by the organisations responsible for the personal data being processed. So, LEAs have a responsibility to ensure that the data and information they collect and process is of high quality.

23 For an overview of measures that can be taken and their origins in the GDPR, see, for instance, this framework: https://www.privacycompany.eu/factsheets/#%2Ffiles%2FPrivacy%2520by%2520Design%2520Framework%2520-%2520English.pdf .
6. Conclusion

6.1 Summary list of Recommendations

This report has highlighted and discussed some of the ethical and legal challenges posed by the policing of the Dark Web. The discussion aims to be responsive to current practices and relevant to key actors in the field, principally LEAs and private actors that contribute to policing on the Dark Web. Though technologies and practices in this area change and develop fast, the report has attempted to focus on issues whose relevance is likely to persist in at least the near future. As far as possible, discussion of issues has been followed up by concrete recommendations for future action, directed to key actors in the field.

The role of national LEAs/police professional bodies in drafting guidance, developing best practice and securing uptake is vital. But international institutions such as Europol and Interpol also play an important role in disseminating best practice. Industry should be the proactive generators of self-regulation and good practice, not only the passive participants of state-led governance.

A number of recommendations have emerged from the discussion in this report. These are directed to LEAs, companies, and to those defining research agendas in this field. These are extracted from the text and reproduced below.

- LEAs should adopt a targeted approach to policing the Dark Web, focusing on exposing, disrupting and prosecuting criminals while refraining from interfering with innocuous activities and the exercise of political freedoms.
- LEAs should put in place strategic and long-term provision of psychological, moral, and professional support for officers involved in operations that bring them close to disturbing activities such as torture and child abuse.
- If in the course of operations LEAs share images or videos of abuse, torture, assassinations or similarly rights-violating actions they should develop a policy on consulting and/or compensating victims whose images are shared and/or, where appropriate, their families.
- LEAs should develop supplementary, detailed guidance for authorizing and covert officers doing operations on the Dark Web in order to ensure that they are carried out in ways that are necessary and proportionate. Guidance should specify considerations to take into account, including: the harm re-victimisation and how to compensate or mitigate it; harms that are related to but fall short of entrapment, such as encouraging, facilitating, and normalizing serious crime; harms to the welfare of officers; and the harm that is done when LEAs allow crimes to occur that could have been prevented by LEA intervention.
- The effectiveness of tactics and operations should be monitored systematically by LEAs over time to create the kind of evidence base on which best practices could be developed. In this respect, it would be desirable to form an international evidence-base and bank of tactics in order to enable the diffusion
of best practices amongst forces across jurisdictions. Interpol could have an important role to play in any such initiative.

- LEAs should be as transparent as possible about the outcomes of operations and how these constitute effectiveness. With respect to existing, well-publicised operations, the forces in question have released rather vague statements about numbers of arrests. But counting the severity of the sentences instead, e.g. number of years of imprisonment, would better track the harms averted than listing the number of individuals arrested or convicted. And efforts should be made to develop evaluation techniques that can measure the currently undervalued disruption effects of methods and operations.

- Research should be carried out to map LEA reliance on the private sector for technical tools and capabilities in investigations online, to assess LEA needs, and to forecast how this is likely to develop in the future. The outcomes of such studies should be used to plan and invest in LEA capabilities in a strategic way.

- LEAs should make sure that means used by private companies they rely on are lawful and that the evidence collected is admissible in court- for example, by establishing an agreement on the way work covered by a contract will be carried out. Such an agreement could cover issues such as a commitment by private companies to use technological methods designed to ensure the integrity of the evidence collected.

- Private companies offering particular services or tools for Dark Web investigations should develop, publish and abide by Codes of Conduct to develop responsible and accountable practice.