Shining a Light on Policing of the Dark Web: An analysis of UK investigatory powers

Gemma Davies: Associate Professor, Northumbria University, UK

Abstract

The dark web and the proliferation of criminals who have exploited its cryptographic protocols to commit crimes anonymously has created major challenges for law enforcement around the world. Traditional policing techniques have required amendment and new techniques have been developed to break the dark web's use of encryption. As with all new technology, the law has been slow to catch up and police have historically needed to use legislation which was not designed with the available technology in mind. This paper discusses the tools and techniques police use to investigate and prosecute criminals operating on the dark web in the UK and the legal framework in which they are deployed. There are two specific areas which are examined in depth: the use of covert policing and hacking tools, known in the UK as equipment interference. The operation of these investigatory methods within the context of dark web investigations has not previously been considered in UK literature, although this has received greater analysis in the United States and Australia. The effectiveness of UK investigatory powers in the investigation of crimes committed on the dark web are analysed and recommendations are made in relation to both the law and the relevant Codes of Practice. The article concludes that whilst the UK has recently introduced legislation which adequately sets out the powers police can use during online covert operations and when hacking, the Codes of Practice need to specifically address the role these investigative tools play in dark web investigations. Highlighted as areas of particular concern are the risks of jurisdiction forum shopping and hacking overseas. Recommendations are made for reform of the Investigatory Powers Act 2016 to ensure clarity as to when equipment interference can be used to search equipment when the location of that equipment is unknown.

Key words

Dark web; darknet; anonymous communication networks; investigatory powers; hacking; equipment interference; network investigative techniques; jurisdication forum shopping; online covert policing;

Introduction

Originally created by the U.S. Naval Research Laboratory to provide a means for military units and field agents to communicate online without being identified and tracked, the dark web[1] is a global network of computers that use a cryptographic protocol to communicate, enabling users to conduct transactions anonymously without revealing their location. You need easily obtained specialised anonymity software to access the dark web. The most commonly used software is The Onion Router Project (or Tor).[2] Strong encryption and anonymity protocols ensure that the IP addresses of the servers that run these sites remain hidden so that the authorities cannot easily identify who is using them, even if they manage to identify an illegal website and place it under surveillance. Whilst it is difficult to ascertain the extent of offending on the dark web, a 2014 study found the most common type of content requested by those using hidden services via Tor was child pornography followed by black marketplaces.[3] Researcher at King's College London found that 57% of the hidden-services websites within the Tor network facilitate criminal activity, including drugs, illicit finance and

[1] Also known as darknet as popularised by U.S. literature such as; Peter Biddle, Paul England, Marcus Peinado and Bryan Willman, 'The Darknet and the Future of Content Distribution', ACM Workshop on Digital Rights Management, 18 November 2002, p. 54, https://crypto. stanford.edu/DRM2002/prog.html <last accessed 24 May 2020>

[2] To access the anonymous sites of the Deep Web, visitors must use a TOR (The Onion Router) browser available at https://www.torproject.org/projects/torbrowser.html.en to access websites with the ".onion" domain

[3] Owen, Gareth and Nick Savage, 'The Tor Dark Net' (2015) Global Commission for Internet Governance, Paper Series No. 20.

pornography involving violence, children and animals.[4] A dark web marketplace or crypto-market is a website operating as a black market selling primarily illegal goods such as drugs, weapons, counterfeit currency, stolen credit card details, forged documents and unlicensed or counterfeit pharmaceuticals. Such marketplaces are characterised by their use of dark web anonymised access, bitcoin payment, and vendor feedback systems modelled on those found on eBay. Once an order has been placed, the buyer transfers the correct amount of Bitcoins to an escrow account, an electronic wallet controlled by the administrator of the web market. When the buyer receives the product, usually through the post, the buyer then notifies the administrator who can release the money to the vendor.

In contrast to surface web browsers, the Tor browser allows users to connect to web pages anonymously by bouncing connections randomly between Tor nodes to obfuscate the IP address of the end user. The anonymity Tor provides makes it an attractive tool for users who wish to engage in illegal activities. Tor software's use of a worldwide volunteer network of relays aims to prevent websites (and Law enforcement) from tracking users and therefore allows users to share information over public networks without compromising privacy. Using the Tor browser '[t]he sender of a piece of traffic will find an entry point and choose a random routing path through a selection of relays to obfuscate their point of origin. Traffic routed along this path will be encrypted until it leaves the last relay, to be sent to a specific IP address on the public Internet.'[5] In the early part of the last decade the Tor system was described as 'so effective that it makes the mass surveillance of ordinary individuals impossible, even if the NSA or local police wanted to try.'[6] Even in 2016 it was argued that there were clear 'legal and technological gaps that exist in law enforcement's ability to cope

[4] Daniel Moore and Thomas Rid, 'Cryptopolitik and the Darknet' [2016] 58(1) Survival 7-38
[5] Danny Bradbury, 'Unveiling the Dark Web' (2014) 4 Network Security 14
[6] Iain Gillespie, Cyber Cops Probe the Deep Web, SYDNEY MORNING HEROLD (Oct. 24, 2013), available at http://www.smh.com.au/digital-life/digital-life-news/cyber-copsprobe-the-deep-web-20131023-2vzqp.html <last accessed March 18 2020>

with and respond to electronic and cyber-crime.'[7] The general consensus in the early part of the millennium was that policing of the dark web was almost impossible due to 'randomness, anonymity and encryption.'[8]

However in the UK, as in most other western jurisdictions the police service were 'acutely aware of the large and growing problem of cybercrime and [were] actively working … nationally and internationally along with the private sector to combat criminality on the web.'[9] As the use of the dark web to commit crime grew exponentially, so did the abilities of Law Enforcement Agencies (LEAs) and cybercrime ascended LEAs' agendas across the world.[10] Neither cybercrime nor the dark web is a threat the UK has been taking lightly. In 2016, the UK launched a 5-year National Cyber Security Strategy that included £1.9 billion of investment and established the National Cyber Security Centre.[11] The UK government also launched the £13.5 million Cyber Innovation Centre in London to help enhance the UK's global reputation in cybersecurity. The UK aims to have a dedicated cybercrime unit in every police force in England and Wales in addition to a national training programme for police, sponsored by the National Police Chiefs Council. This is not just a UK response but a worldwide police response with Europol creating the European Cybercrime Centre (EC3) in 2013. Specific dark web responses are slower but can now be seen. In 2015 the UK announced a dedicated unit for tackling dark web crime called 'Joint Operations Cell' or JOC. This is a joint, co-located initiative between the National Crime Agency (NCA) and Government Communications Headquarters (GCHQ) which initially is to focus on child sexual exploitation and is aimed at ensuring 'no part of the internet, including the dark web, can be used with impunity by criminals to conduct

[7] Senya Merchant, COPS office, How the Web Presents New Challenges for Law Enforcement Agencies, Jan. 2014

[8] Taylor Armerding, 'To Shine a Light on Cybercrime', Go Dark, 10 August 2015 https://www.csoonline.com/article/2960728/to-shine-a-light-on-cybercrime-go-dark.html <last accessed March 18 2020>

[9] Adrian Goldberg, The Dark Web: Guns and Drugs for Sale on the Internet's Secret Black Market, BBC news (Feb. 3, 2012), http://www.bbc.com/news/business-16801382 <last accessed March 18 2020>

[10] David Wall and Matthew Williams, 'Policing Cybercrime: networked and social media etchnologies and the challenges for policing' (2013) 24(4) Policing and Society 409-412

[11] National Cyber Security Centre, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do <last accessed March 18 2020>

their illegal acts.'[12] In 2018 Europol created its own dedicated dark web team[13] and the US Justice Department created the Joint Criminal Opioid Darknet Enforcement Team known as J-Code.[14]

This paper discusses the tools and techniques police use to investigate and prosecute criminals operating on the dark web. The first part of the article briefly considers investigative techniques which are traditional in nature but have proved effective in dark web investigations. The second part of the article considers two techniques in much more depth: the use of covert policing and hacking tools. The use of these techniques within the context of dark web investigations has not previously been considered in UK literature although this has received greater analysis in the United States and Australia. Both techniques are considered from the UK perspective and the law which governs their use is set out. The aim of this article is to consider the effectiveness of UK investigatory powers in the context of investigations of crimes committed on the dark web. This is an area of policing which receives very little consideration but is of growing importance. By shining a light on this little understood corner of policing the legal framework UK police must operate within is analysed and recommendations are made for reform.

Policing the dark web

[12] GCHQ, https://www.gchq.gov.uk/news/gchq-and-nca-join-forces-ensure-no-hiding-place-online-criminals <last accessed March 18 2020>
[13] Europol, https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure <last accessed March 18 2020>
[14] United States Department of Justice, Press Release: 18-110 (19 April 2020) https://www.justice.gov/opa/pr/attorney-general-sessions-announces-new-tool-fight-online-drug-trafficking <last accessed March 18 2020>

The first step in identifying a suspect online is to trace the Internet Protocol (IP) address. This is not possible when an individual has accessed a site through a dark web browser such as Tor. A user needs no specialist knowledge or equipment to download or access sites using Tor so with a minimum level of technical expertise any individual with a computer and access to the internet can become unidentifiable to LEAs who are using traditional investigative techniques to unmask a user's IP address. Most LEAs and the UK's intelligence and security communities remain understandably secretive in relation to the tools and techniques used to unmask dark web criminals. Whilst there is no definitive list of all policing techniques used to investigate crimes committed on the dark web it is possible from publicly available information to see which techniques are most often used. Whilst the dark web has historically been portrayed as a space beyond the reach of law enforcement, where criminals are protected by a veil of technological anonymity, this is no longer the reality. Police all over the world, including the UK, have deployed a wide array of different techniques to identify, arrest and convict drug dealers, weapon buyers, child pornographers, terrorists and other criminals.[15]

One of the most commonly used policing techniques in all cyber investigations, including those on the dark web is the use of Open Source Intelligence. OSINT is data and information that is collected legally from open and publicly available resources. Obtaining the information doesn't require any type of clandestine effort and it is retrieved in a manner that is legal and meets copyright requirements. There are a wide range of OSINT tools available, some of which are specific to the dark web.[16] OSINT sources require police officers to scour the web for breadcrumbs of information which lead to unmasking identities usually left through human error. This can come from forum posts in web-based communities, user generated contact, social networking sites, wikis, blogs and

[15] Joseph Cox, Motherboard (26 June 2016) https://www.vice.com/en_us/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web <last accessed March 18 2020>
[16] Jake Creps (16 May 2019) https://jakecreps.com/2019/05/16/osint-tools-for-the-dark-web/ <last accessed March 18 2020>

news sources, amongst others. The Investigatory Powers Commissioner's Office 2018 annual report noted that 'internal oversight of open source activity was inadequate' and the IPCO expected to see improvement by the next inspection.[17] Poor recording of OSINT activity can lead to problems in complying with disclosure in a subsequent prosecution and/or a failure to recognise when activity requires a directed surveillance authorisation, as discussed below. Cybercriminals must find a balance between masking their identity in order to evade law enforcement and leaving part of their identity unmasked in order to attract potential criminal collaborators and 'customers'.[18] Jonathan Lusthaus has detailed the tensions inherent in developing an online identity which require criminals to 'attempt to pierce the veil of anonymity that the internet affords them, but not discard it entirely'.[19] The more notorious an online moniker or pseudonym becomes the more profitable their illegal enterprises are likely to be but conversely the more likely it is that they will attract the attention of law enforcement agencies. One of the largest dark web marketplaces, Silk Road was ultimately taken down as a result of open source information. The Silk Road in its very early stage had been advertised on a bitcoin forum using a personally identifiable email address. This led to the arrest and ultimately successful prosecution of Ross Ulbricht known by the pseudonym Dread Pirate Roberts in the United States.[20] He was given five concurrent sentences including two of life imprisonment without the possibility of parole.[21] Another prolific dark web drug dealer, David Ryan Burchard, was arrested after he tried to trademark his dark web brand 'caliconnect' in his own name.[22] This case demonstrates that online identities are effectively the brand of a cybercriminal. It is the foundation of their reputation and therefore there is an incentive to maintain that identity or a

[17] IPCO 2018 at [11.28 – 11,29]
[18] Jonathan Lusthaus, 'Trust in the World of Cybercrime' [2012] 13(2) Global Crime 71-94
[19] Jonathan Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime* (1st ed, Harvard University Press, Massachusetts, 2018) pg 106
[20] Donna Leinwand Leger, USA Today, 15 May 2014 How the FBI brought down Cyber-underworld site Silk Road, https://eu.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/ <last accessed March 18 2020>
[21] Andy Greenbery, WIRED (31 May 2017) https://www.wired.com/2017/05/silk-road-creator-ross-ulbricht-loses-life-sentence-appeal/ <last accessed March 18 2020>
[22] Joseph Cox, Motherboard (30 March 2016) https://www.vice.com/en_us/article/9a3a4d/suspected-dark-web-vendor-charged-after-trying-to-trademark-his-brand-caliconnect <last accessed March 18 2020>

close variation of it - a fact which LEAs can use to their advantage. A second, closely related technique is the interrogation of seized data. Successful arrest or seizure of a dark web marketplace can generate additional leads for police investigators. The German drugs vendor 'Shiny Flakes' for example had kept a spreadsheet of all customer orders which was used by police to track down his buyers.[23] Thirdly, despite the use of Bitcoin transactions to purchase items bought on the dark web it is still possible for authorities to track buyers and sellers '[b]y examining the pattern of transactions, the authorities may be able to tie a Bitcoin transaction to a real-world identity.'[24] David Burchard was initially investigated because of his sale of millions of dollars of bitcoin to an unlicensed currency exchange.[25] Blockchain evidence was present at the trial of Shaun Bridges, a U.S. secret agent who stole $820,000 worth of bitcoin while investigating the Silk Road. At the trial, prosecutors presented a diagram which mapped out how thousands of bitcoins were funnelled from Silk Road into a Mt Gox account which belonged to Shaun Bridges, allowing police to follow wire transfers to a company created by him. Finally, no matter how sophisticated your encryption, if you are dealing in physical goods, such as drugs or guns, offenders have to have some sort of delivery system. This is the point at which goods can be intercepted and potentially seized by customs officials. Law Enforcement may then set up surveillance to monitor who is picking up or posting such items or make a controlled delivery.

Going undercover on the dark web

[23] Unknown, Accused Shiny Flakes Customer: "Everyone Could Use My Address" (02 August 2017) https://thebitcoinnews.com/accused-shiny-flakes-customer-everyone-could-use-my-address/ <last accessed 18 March 2020>

[24] Timothy lee, The dark web: what it is, how it works, and why it's not going away (31 December 2014) https://www.vox.com/2014/12/31/7470965/dark-web-explained <last accessed 18 March 2020>

[25] Department of Justice, U.S. Attorney's Office, Press release (29 March 2016) https://www.justice.gov/usao-edca/pr/merced-man-arrested-distributing-marijuana-and-cocaine-nationwide-through-silk-road-and <last accessed March 18 2020>

Undercover policing is certainly not a new or novel method of policing and online undercover policing has also been used for some time in cyber investigations. However, the ability of police to infiltrate online forums in order to obtain evidence required for a successful prosecution is essential when tracking anonymous users on the dark web.[26] Infiltrating online forums requires police to establish a controlled surveillance operation in which officers covertly act as administrators or moderators of illicit forums.[27] Online undercover operations require a significant degree of skill as officers must learn to mimic the patterns and style of online personas they are impersonating and this represents a significant investment of time and resources for LEAs. One of the main priorities of undercover LEAs is investigating chat rooms, newsgroups, and peer-to-peer networks. Agents enter forums posing as offenders requesting images from others, or they enter groups posing as children to lure out the paedophiles in the group.

Such operations have been very successful. For example, in the U.S. a LEA covertly took over the account of a staff member on the Silk Road and continued to work undercover whilst the site was taken over by police. Maintaining cover during this period enabled the officer to be invited to participate in the creation of the second Silk Road. Another dark web marketplace, Hansa, was one of the largest dark web markets in Europe. During Operation Bayonet, the Netherland National High-Tech Crime Unit (NHTCU) installed network monitoring equipment which eventually led them to the Tor protected server that ran Hansa. Instead of shutting the site down as had been done before they chose to continue to operate the site for one month with officers posing as the administrator of the site. At the same time, the FBI located one of the servers of Alphabay, one of the largest dark web drug markets in the world. NHTCU timed their takeover of Hansa to coincide with the FBI take down of Alphabay. This resulted in 5000 users a day flocking from Alphabay to Hansa all of whom fell

[26] Elizabeth Joh, 'Breaking the law to enforce it: Undercover police participation in crime' [2009] 62(1) Stanford law Review 239-273

[27] Jonathan Lusthaus, 'Trust in the World of Cybercrime' [2012] 13(2) Global Crime 71-94

under surveillance. Over 27 days NHTCU collected information on over 27,000 transactions and obtained data on 420,000 users including 10,000 home addresses.[28]

In order to maintain an effective undercover operation officers are required to gain and maintain trust. That officers are not allowed (or empowered) to perform criminal acts is recognised by criminals as an effective signal of an undercover operation. This equally applies to online undercover operations. Lusthaus describes criminal acts as an important step in validating online identity amongst cybercriminals.[29] The example of DarkMarket is given. The site required prospective members to provide details of 100 compromised credit cards, which would then be tested by two reviewers who would report on whether the individual should be trusted to join the organisation. A controversial aspect of undercover work surrounds the extent to which an undercover officer can engage in activity that would otherwise be illegal. Before turning to the way such operations are regulated in the UK it is helpful to discuss the high-profile Australian police unit called Taskforce Argos. The regulations governing the use of police powers differ between Australian states which are each their own jurisdiction. The state of Queensland has more expansive powers in relation to covert intelligence gathering operations than other states and indeed most western jurisdictions. The Police Powers and Responsibilities Act 2000 allows Queensland officers to apply to the courts for permission to commit criminal offences in the course of an investigation. Taskforce Argos can petition the court to allow officers to disseminate child exploitation material during online covert operations in order to maintain cover. According to Bleakley:

> the Queensland child exploitation unit has become an integral participant in many multinational investigations conducted into the supply of child exploitation material on the Dark Web; its position at the centre of several major covert operations makes Taskforce

[28] Andy Greenbery, WIRED (03 August 2018) https://www.wired.com/story/hansa-dutch-police-sting-operation/ <last accessed 18 March 2020>
[29] Jonathan Lusthaus, 'Trust in the World of Cybercrime' [2012] 13(2) Global Crime 71-94

> Argos the perfect framework through which it is possible to understand the implications of using covert tactics when investigating potential criminal offences in a digital environment.[30]

Taskforce Argos's involvement in overseas operations is well documented and long standing. They were involved in collaboration with the FBI in 2006 during Operation Achilles and with the Canadian police in 2014 during Operation Rhodes. In 2016 Operation Artemis focused on two interconnected child exploitation forums on the dark web: Giftbox Exchange and Child's Play. This operation was initially run in conjunction with an unspecified European law enforcement partner and led to the arrest of Patrick Falte and Benjamin Faulkner in the United States. Law enforcement were able to obtain the passwords for Child's Play from Faulkner which were then passed on to Taskforce Argos who took over as administrator of the site. In order to maintain cover, police had to post a monthly status update which had to include an image of child exploitation to 'prove' to members that the site was not compromised. This activity would not have been legal in the U.S. and therefore police had to collaborate with Taskforce Argos in Australia. The site was operated for 11 months before shutting down but the operation successfully identified 90 primary targets worldwide and over 900 users.[31] The ability to act across jurisdictional borders, anywhere in the world, is given to Queensland police under the provisions governing controlled operations in the Police Powers and Responsibilities Act 2000; there is no condition in this act that officers must reasonably believe an offence is being committed or will be committed in Queensland, giving specialist teams like Taskforce Argos the authority to act outside of its jurisdiction in 'a loosely-defined range of situations'.[32]

Forum shopping is a term applied when multiple courts have concurrent jurisdiction over a claimant's claim, with a claimant choosing to bring a claim in the most favourable jurisdiction. Whilst forum shopping is usually associated with civil cases it is a term which can be applied in relation to

---

[30] Paul Bleakley, 'Watching the watchers: Taskforce Argos and the evidentiary issues involved with infiltrating Dark Web child exploitation networks ' [2019] 92(3) The Police Journal: Theory, Practice and Principles 221-236

[31] Hoydal, HF, Stangvik, OS, Hansen, NR, Breaking the Dark Net: Why the police share abuse pics to save children. VG (07 October 2017) Available at: www.vg.no/spesial/2017/undercover-darkweb/ <last accessed 18 March 2020>

[32] Paul Bleakley, 'Watching the watchers: Taskforce Argos and the evidentiary issues involved with infiltrating Dark Web child exploitation networks ' [2019] 92(3) The Police Journal: Theory, Practice and Principles 221-236

prosecution form shopping. In this scenario, in a case of concurrent jurisdiction prosecutors choose to proceed to prosecution in a jurisdiction with favourable rules of evidence or a harsher sentencing regime.[33] It should be noted that there are a range of national and bilateral guidelines applicable in cases of concurrent jurisdiction which aim to ensure prosecutions occur in the most appropriate jurisdiction, usually defined as where most of the harm or most of the offending occurred.[34] A term more aptly applied to Taskforce Argos's significant involvement with overseas operations is 'jurisdiction forum shopping'. In this scenario LEAs seek to move their investigation in order to take advantage of the laws of another jurisdiction which are favourable to their investigation. At its extreme, as seen in Operation Artemis, this can be used to move an investigation to a jurisdiction which will allow an investigative technique which would be unlawful in the originating jurisdiction. When dealing with offending occurring through the dark web this would in no way impact on the originating state's ability to prosecute as it is likely that harm will (also) have occurred in that state and that concurrent jurisdiction is therefore held by multiple countries. This is a phenomenon which has received very little critical analysis either by academics or LEAs.[35] Such operations have been described as falling into a 'gray area' which could be 'considered a collaborative partnership or a case of jurisdictional forum shopping by international law enforcement agencies'. Bleakley, an Australian academic, states that 'the collaborative partnerships that exist between Taskforce Argos and its international counterparts indicates that a lack of clearly-defined sovereignty has in fact proven beneficial in the pursuit of online child exploitation networks.' Despite this he argues that 'good faith' principles can be applied to allow for the evidence to be used by international partners.[36]

---

[33] Frank Zimmermann, 'Conflicts of Criminal Jurisdiction in the European Union' [2015] 3(1) Bergen Journal of Criminal Law and Criminal Justice 1-21

[34] Paul Arnell and Gemma Davies. 'The Forum Bar in UK Extradition Law: an Unnecessary Failure' [2020] forthcoming, The Journal of Criminal Law

[35] There is a brief discussion of this concept in: Trine Thygesen Vendius, 'Proactive Undercover Policing and Sexual Crimes against Children on the Internet' [2015] 2(2) European Review of Organised Crime 6-24 and Paul Bleakley, 'Watching the watchers: Taskforce Argos and the evidentiary issues involved with infiltrating Dark Web child exploitation networks ' [2019] 92(3) The Police Journal: Theory, Practice and Principles 221-236

[36] Bleakley ibid.

Whilst there is no evidence that UK LEAs have ever participated in jurisdiction forum shopping, defined as purposefully collaborating with an overseas LEA as a way of circumventing national rules relating to the conduct of an investigation, UK convictions have resulted from Operation Artemis. In December 2014 Richard Huckle, a UK citizen living in Malaysia, was arrested at Gatwick airport and subsequently sentenced to a minimum of 25 years' imprisonment for 71 offences which included rape against children aged between six months and 12 years between 2006 and 2014[37]. Evidence against Huckle was collected by Taskforce Argos and passed to the National Crime Agency.[38] Other high-profile UK prosecutions also reveal cooperation between UK police and LEAs outside the UK. Matthew Falder was convicted in the UK of 135 sexual offences in October 2017 but was initially identified by the FBI in August 2013 during an operation which saw them build their own website on the servers which hosted illegal sites to track what was being said and done on them. In doing so they accessed the website 'Hurt 2 The Core' where amongst images of rape, murder, sadism, torture, paedophilia, blackmail and humiliation a user posted a blackmail picture of a teenage girl who was tracked to posts on a classified advertisement website on the clear web. At the same time one of Falder's pseudonyms also came to the attention of the NCA in the UK. A special task force was set up involving the NCA, GCHQ, Homeland Security in the US, the Australian Federal Police and Europol with help from law enforcement in Israel and Slovenia to 'enhance evidence gathering against the suspect'[39]. Exactly what is meant by this phrase is not clear and potential issues relating to disclosure could arise.[40] Similar transnational operations have also been used to convict drug offenders. In 2018, a group of University of Manchester students led by Basil Assaf were jailed for

[37] Karen McVeigh, The Guardian, Richard Huckle given 22 life sentences for abuse of Malaysian children (06 June 2016) https://www.theguardian.com/uk-news/2016/jun/06/richard-huckle-given-23-life-sentences-for-abusing-malaysian-children <last accessed 18 March 2020>

[38] Michael Safi, The Guardian, The Takeover: how police ended up running a paedophile site (13 July 2016) https://www.theguardian.com/society/2016/jul/13/shining-a-light-on-the-dark-web-how-the-police-ended-up-running-a-paedophile-site <last accessed 18 March 2020>

[39] Jessica Labhard, BBC, Matthew Falder: How global taskforce caught Birmingham paedophile https://www.bbc.co.uk/news/uk-england-birmingham-42921977 <last accessed 18 March 2020>

[40] Chrisje Brants, Adam Jackson and Tim Wilson, A comparative Analysis of Anglo-Dutch approaches to "cyber policing": checks and balances fit for purpose? In this special edition

up to 15 years and three months for selling £800,000 worth of drugs on the Silk Road. Information relating to their arrest is presumed to have come from the FBI as their arrest coincided with the day the FBI shut down the Silk Road in October 2013.[41]

What if UK police did engage in jurisdiction forum shopping and the admission of evidence obtained was subsequently challenged in a UK court? Such a discussion must be theoretical as no such case has come before UK courts. Bleakley opined that the use of evidence obtained by Taskforce Argos and then passed to and used for prosecution purposes by a foreign LEAs could have significant ramifications and 'result in putting children at a greater level of risk caused by criminal trials being thrown out.'[42] To what extent is that an accurate representation of the law in the UK? There are two ways of looking at this question. Firstly, the approach of the courts to excluding evidence on the grounds of fairness and secondly the approach of the courts to staying proceedings on the grounds of abuse of process.[43] Turning to the former, the approach to unlawfully obtained evidence in England and Wales is that such evidence is prima facia admissible but is subject to exclusion on the grounds of fairness through the general discretion to exclude prosecution evidence found in section 78 of Police and Criminal Evidence Act 1984. This states that in any proceedings the court may:

> refuse to allow evidence on which the prosecution proposes to rely if it appears to the court that, having regard to all of the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.

Deliberately taking over the running of an existing illegal site for the purpose of monitoring users who are then brought under surveillance would be unlikely to result in the exclusion of that

[41] Josh Halliday, Manchester students jailed for selling £800k of drugs on dark web, The Guardian (21 March 2018) https://www.theguardian.com/uk-news/2018/mar/21/manchester-students-jailed-selling-800k-drugs-dark-web <last accessed 18 March 2020>
[42] Bleakley, n.32
[43] See Brants, Jackson and Wilson n.40

evidence in the UK. It seems therefore also likely that using such evidence obtained from an overseas LEA would also not result in exclusion. This approach is confirmed by the case of Khan[44] where the trial court declined to exclude evidence obtained by police use of a secret listening device even though at the time there was no statutory code to govern the use of such covert surveillance. The case eventually made its way to the European Court of Human Rights which held that this did not constitute a breach of Article 6 of the European Convention of Human rights as the central question was whether the proceedings 'as a whole' were fair.[45]

A second possible argument would be to request a stay of proceedings for abuse of process possibly on the grounds that the continued operation of the website/forum amounted to state entrapment. The main authority in England on state entrapment is R v Looseley[46] where Lord Nicholls confirmed that the main remedy for state entrapment cases was the granting of a stay under the abuse of process doctrine.[47] The test however is set very high and requires 'the involvement of the court in the conviction of the defendant … would compromise the integrity of the judicial system', be 'an affront to the public conscience' and thus bring 'the administration of justice into disrepute'.[48] Whilst the court would take into account the nature of the offence and the reason for the operation it would appear that in the absence of bad faith such an application would be unlikely to be successful.[49]

[44] Khan v the United Kingdom (2001) 31 E.H.R.R. 45
[45] Ibid at [38] "The Court notes that at each level of jurisdiction the domestic courts assessed the effect of admission of the evidence on the fairness of the trial by reference to section 78 of PACE, and the courts discussed, amongst other matters, the non-statutory basis for the surveillance. The fact that the applicant was at each step unsuccessful makes no difference."
[46] R v Looseley, AG's reference (no 3 of 2000) [2001] UKHL 53
[47] This was reaffirmed in the case of R v Latif [1996] 1 ALL ER 353 (HL)
[48] Looseley n 46 at [31] (Lord Hoffmann)
[49] Alisdair A. Gillespie, 'Paedophile hunters: how should the law respond?' (2010) 12 Crim. L.R. 1016-1034

The question that follows from this assessment is whether it would ever be appropriate for UK LEAs to engage in jurisdiction forum shopping in light of jurisprudence which suggests that such evidence would not be excluded by UK courts. This paper argues that jurisdiction forum shopping is not a tactic which is legitimate, even if it is not unlawful. If the UK legislature has decided, on democratic principles, to circumscribe police powers it is difficult to see how it could ever be appropriate for a LEA to circumvent this by moving part of an investigation 'off shore' so that they can benefit from a more permissive investigatory powers. Whilst collaboration with LEAs outside of the UK is a necessary part of investigating dark web crimes where networks inevitably stretch across borders, such engagement should be clearly on the basis of good faith. Whilst UK police have a duty to act on intelligence which is passed to them from overseas LEAs and collaborative operations may become necessary when an investigation is of interest to LEAs in multiple countries, they should not seek to obtain evidence by asking a foreign LEA to undertake investigations as a means of evading safeguards which apply under English law. It would not be justifiable for UK police to use Taskforce Argos in the way the FBI seem to have done. To deliberately seek the help of police in another jurisdiction, not because the crime had links to that jurisdiction, but because police can use investigation tactics which are not available in the UK, would entirely circumvent the 2000 Act and undoubtedly undermine confidence in UK policing. There is no evidence that any UK LEA has engaged or would engage in such conduct. However for the purposes of clarity and trust in UK policing the relevant Codes of Practice should be amended to explicitly state that such a practice is not permissible.[50] Such an inclusion would not only help to clarify the position for those in LEAs but would offer an additional level of protection to UK citizens who fall foul of jurisdiction forum shopping. Whilst a breach of the Code of Practice would not result in a successful application to stay proceedings or a successful application to exclude evidence under section 78 of PACE per se, it would likely be considered by the courts as akin to a breach of the PACE Codes of Practice. In the

[50] See below n [64] for discussion of concerns relating to UK police undercover operations which highlight the importance of comprehensive oversight of undercover operations

Court of Appeal decision of R v King[51] the court, whilst denying the appeal, acknowledged that a deliberate breach of the PACE Codes of Practice is capable of rendering inadmissible evidence obtained as a result of that breach although it would still depend on the factual circumstances of the case as to whether this amounted to unfairness.

Whilst UK police have shared information with Taskforce Argos to what extent would the tactics used by the specialised unit be permissible in the UK? In the UK, if the study of an individual's online presence becomes persistent then authorisation under the Regulation of Investigatory Powers Act 2000 (the 2000 Act) may be needed and officers should adhere to the associated Codes of Practice designed to ensure compliance with the European Convention of Human Rights, in particular Article 8.[52] Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered. Directed surveillance must be both proportionate and necessary. It is necessary if, amongst other things, it is 'for the purpose of preventing or detecting crime or preventing disorder.'[53] Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a Covert Human Intelligence Sources (CHIS) authorisation may be needed.[54] Section 27 of 2000 Act states that conduct shall be lawful for all purposes if 'an authorisation under [the Act] confers an entitlement to engage in that conduct on the person whose it is and his conduct is in

[51] R v King [2012] EWCA Crim 805

[52] Home Office, Covert Surveillance and Property Interference Code of Practice (August 2018) and Covert Human Intelligence Sources Revised Code of Practice (August 2018), available at https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice <last accessed 18 March 2020>

[53] Section 28(3) Regulation of Investigatory Powers Act 2000

[54] Such sources can be both in and outside of the UK. According to paragraph 4.10 of the Covert Human Intelligence Sources Revised Code of Practice (August 2018): members of foreign law enforcement or other agencies or CHIS of those agencies may be authorised under the 2000 Act in the UK in support of domestic and international investigations. When a member of a foreign law enforcement agency is authorised in support of a domestic or international investigation or operation the manual says that "consideration should be given to authorising the individual at the level prescribed by the 2013 Relevant Sources Order as if the individual holds an 'office, rank or position' with an organisation listed in the same Order."

accordance with the authorisation'. The legal limits of section 27 are therefore exceptionally wide and only circumscribed by the tests of necessity and proportionality. No further mention is made of section 27 in either of the Codes of Practice. It therefore appears that as a matter of law there is nothing which would prevent UK police officers from conducting an online undercover operation which could include the distribution of illegal pornography in order to maintain cover. The only other publicly available document which provides any relevant guidance is the Undercover Police Guidance which is still in a draft format despite a consultation closing in 2016.[55] The guidance acknowledges that whilst authorisations should make the parameters of undercover operatives conduct clear, it may be necessary to participate in the criminal activity about which they have been asked to report. The guidance states that the case of R v Looseley 'has identified the limits of acceptable law enforcement conduct' in relation to officers participating in criminal activity but that in addition officers should not engage in planning and committing the crimes, only play a minor role and participate only where essential.[56] Online operations are only very briefly mentioned at the end of the document and no substantive aspect of online deployment is considered.[57]

The failure to adequately address the needs of online undercover operations raises a number of key issues. Firstly, it is argued that the case of Looseley does not adequately deal with the parameters of section 27 as suggested by the draft Undercover Police Guidance. It instead sets out the principles to be considered by the court when invited to stay proceedings as an abuse of process on the grounds of state entrapment. Whilst conduct which would otherwise be criminal may form part of conduct said to amount to entrapment this is not an essential ingredient of entrapment. As such the case of Looseley does not work well for understanding the parameters of conduct which can be authorised under the Act notwithstanding that it would otherwise constitute a criminal offence. More

[55] Available at https://www.college.police.uk/News/College-news/Pages/undercover-policing-guide.aspx <last accessed 23 April 2020>
[56] Ibid paragraph 7.14.1
[57] Ibid paragraph 11.3

specifically it is of limited use to officers trying to understand the legitimate parameters of online covert investigations more generally.[58] The lack of attention given to undercover online operations in all policy and professional practice documents was noted in a 2014 HMIC report which concluded that police were hindered by there being no nationally agreed definition of undercover online officers, effective recognition of the role in key policy documents and insufficient training which addressed the specific problems associated with online deployment.[59] The report also noted that only 25 out of 44 forces had a dedicated undercover online capability and forces seemed not to appreciate the importance of the extent of the cybercrime threat and the need to employ undercover online tactics to meet those challenges.[60] This assessment accords with the research team's experience during interviews and interactive workshops which revealed that whilst some undercover tactics are employed within the UK this is generally the reserve of the National Crime Agency and a few highly specialised teams. Online undercover operations are an underutilised tactic within the rest of UK policing. This is not because such tactics are circumscribed by the law but because of a lack of expertise, resources and clarity in policy and Code of Practice documents has resulted in an overly cautious approach by local cybercrime units.

Between 1 October 2011 and 30 September 2013 there were 354 undercover online operations authorised in the UK.[61] The Investigatory Powers Commissioner's Office produces an Annual Report which must include statistics on the use of the relevant investigatory powers. The report for 2018 was published in early 2020 but does not differentiate between online and offline authorisations. The report sets out that the number of authorised CHIS has gradually declined over the last ten years

[58] Giollabhuí, Goold, and Loftus 'Watching the watchers: conducting ethnographic research on covert police investigation in the United Kingdom' (2016) 16(6) Qualitative Research 630-645
[59] HMIC, An Inspection of Undercover Policing in England and Wales (2014) available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/an-inspection-of-undercover-policing-in-england-and-wales.pdf <last accessed 23 April 2020>
[60] Ibid at para [114]
[61] HMIC, An inspection of undercover policing in England and Wales (2014) ISBN: 978-1-78246-515-7, para [26] available at https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/an-inspection-of-undercover-policing-in-england-and-wales.pdf <last accessed 18 March 2020>

with only 124 CHIS authorisations granted to LEAs in 2018.[62] There were however 6,108 directed surveillance warrants issued to LEAs although again there is no further break down of this number. Despite the overall decrease in the number of CHIS authorisations the IPCO 2018 Annual Report notes a 'growth of online activity' and that correspondingly LEAs have introduced a 'range of training to allow staff to lawfully exploit this source of information' although some agencies have been slower to build their online capabilities. It is important that the extent to which these powers are used to authorise online covert surveillance and the extent to which such operations permit officers to engage in activity which would otherwise be illegal is properly understood. The IPCO annual report should break down the figures so that the extent to which LEAs use the powers to authorise online undercover operations is known and the public can have confidence that these powers are monitored and effectively overseen.

Undercover policing has been described as a "necessary evil" because of its potential for misuse. By their very nature, covert methods are subject to abuse and to the avoidance of accountability.[63] In the UK a number of well publicised scandals relating to the conduct of officers whilst undercover[64] have resulted in a series of reviews including an ongoing Undercover Policing Inquiry.[65] The nature of undercover policing (both online and offline) and the inevitable secrecy of its operation heightens the risk of misuse. When this is combined with a lack of recognition of online undercover investigations in policy and practice document, a lack of training and a seeming reticence to clearly set out boundaries for police engaged in such work the risks for officers and to public confidence are

[62] The report suggests this decline corresponds to a decline in available resources.
[63] Grabosky & Gregor, 'Online Undercover Investigations and the Role of Private Third Parties' (2019) 13(1) International Journal of Cyber Criminology 38-54
[64] HMIC, An Inspection of Undercover Policing in England and Wales (2014) There have been widespread concerns about undercover policing for a number of years. See paragraph 5 and 6 "Allegations that undercover officers have had sexual relationships with those who are linked with the target of their investigations, that they have given false evidence in court to maintain their undercover status, and that they have used the details of children who have died as their covert identities have all contributed to a growing unease that the tactic is being wrongly used, badly supervised, and ineffectively controlled."
[65] Undercover Policing Inquiry available at https://www.ucpi.org.uk/about-the-inquiry/ <last accessed 18 March 2020>

manifest. There is no universally accepted approach in covert investigative methods used in active investigations of online child exploitation. Australian courts have taken a very liberal approach[66] whilst in New Zealand the Principles of Practice for Investigating on-Line Grooming of Children Under 16 preclude the transmission of 'objectionable images'.[67] Joh argues from a U.S. perspective that 'authorised criminality' is 'secret, unaccountable, and in conflict with some of the basic premises of democratic policing' and therefore undermines social support for the police.[68] Alternatively academics such as Yar argue that the policing of sexual offences on the internet occupies an anomalous position as such crimes have a 'higher hierarchy of standing' in relation to other internet crimes as perceived in public, political and media consciousness.[69] From a European perspective child exploitation is one of the three main priorities of Europols 'European Cybercrime Centre' (EC3). Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children further prescribes that the EU Member States shall 'ensure that sexual offences against children are effectively investigated'. Vendius argues that undercover policing is a necessary investigative tool in order to detect and infiltrate child pornography networks.[70] There are a number of EU countries which allow for undercover online investigations to authorise police to act as a 'participating offender' in order to infiltrate an organisations which include Belgium and the Netherlands. Vendius's research suggests that the UK does allow officers to share child pornography when necessary but one interviewee stated that 'most senior officers would say no to the sending of images on the grounds of further victimisation rather than being illegal'.[71] A decision as to whether such conduct is appropriate should not be made by individual officers but should have been clearly

[66] R v Stubbs [2009] ACTSC 63 (26 May 2009)
[67] New Zealand Police, Principles of Practice for Investigating On-Line Grooming of Children Under 16. Reproduced in R v Stubbs [2009] ACTSC 63
[68] Elizabeth Joh, 'Breaking the law to enforce it: Undercover police participation in crime' [2009] 62(1) Stanford law Review 239-273. The article defines authorised criminality as 'the practice of permitting covert police officers to engage in conduct that would be criminal outside of the context of the investigation'
[69] Majid Yar, 'The policing of Internet sex offences: pluralised governance versus hierarchies of standing' (2013) 23(4) Policing and Society 482-497
[70] Vendius, T. T. 'Proactive Undercover Policing and Sexual Crimes against Children on the Internet' (2015) 2(2) European Review of Organised Crime
[71] Ibid page 16

considered at a national level and communicated to all officers engaged in undercover operations. Despite Vendius's research the extent to which UK LEAs engage in conduct such as that seen by Taskforce Argos in Operation Artemis is unknown and therefore lacks transparency. As a minimum publicly available guidance for online undercover operatives is needed urgently. This is an issue which should sensibly form part of the ongoing Undercover Policing Inquiry.

Law Enforcement Agencies use of hacking in a dark web context

The dark web operates in a way which makes activity easy to see but the identity of those involved hard to reveal. In many instances, despite the use of various techniques described above, law enforcement agencies can observe dark web users committing crimes but cannot identify them for further investigation and prosecution without hacking[72] into their computers.[73] Such hacking constitutes a search, which means law enforcement must obtain authorisation beforehand. Law enforcement use of online hacking is referred to by different names in different jurisdictions. In the U.S. it is commonly described as Network Investigative Techniques (NITs) or Computer Exploitation. In the UK it is more commonly referred to as Equipment Interference as defined in the Investigatory Powers Act 2016. Such techniques are particularly needed in dark web investigations where suspects are using anonymising software such as Tor to obscure their location. The International Association of Chiefs of Police reports that LEAs are "not able to investigate illegal activity and prosecute criminals effectively without evidence collected using hacking techniques."[74] In order to

[72] European Parliament, Directorate-General For Internal Policy, Legal Frameworks for Hacking by law Enforcement: Identification. Evaluation and Comparison of Practice (2017). See page 8 "Although the term 'hacking' is not used by law enforcement agencies, these practices essentially mirror the techniques used by hackers (i.e. exploiting any possible vulnerabilities – including technical, system and/or human vulnerabilities – within an information technology (IT) system)"

[73] Diana Benton, 'Seeking Warrants for Unknown Locations: The Mismatch between Digital Pegs and Territorial Holes' (2018) 68 Emory LJ 183

[74] IACP Summit Report, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence (2015)

unmask a device's identifying information, which will lead to its physical location, and then potentially the user's identity, LEAs use hacking tools which enable them to remotely access and install malware on a computer without its owners' permission.[75] Frequently this is done with the intention of accessing the target computer and converting it into a surveillance device thus circumventing the need to know a target's location. Once installed the malware can cause a computer to perform any task, even forcing it to covertly upload files to a server controlled by law enforcement or instruct the computer's camera or microphone to collect sound and images.

A number of high-profile cases have documented LEAs use of hacking tools around the world. From a U.S. perspective during the investigation of Playpen, a child pornography site, the FBI deployed malware which once clicked by a user revealed their IP address.[76] The operation ran for 13 days and harvested over 1000 IP addresses not only in the U.S. but all over the world.[77] The National Security Agency (NSA) have also deployed a malware named EgotisticalGiraffe to infect users with malware if they download Tor through an outdated web browser allowing them to monitor a downloader's activity.[78] In April 2017 a group called the Shadow Brokers released details of hacking tools alleged to be from the CIA that allow spying on money transfers.[79] In 2016 the Australian authorities used a phishing attack to bypass Tor software as part of a child pornography investigation which allowed them to remotely hack a computer in Michigan.[80] Information found through hacking has also been used in the UK. The Snowdon disclosures revealed that in 2011 GCHQ used a Distributed Denial of

[75] Ibid page [8] alternatives to hacking include "requiring users to provide their password or decrypt their data; requiring technology vendors and service providers to bypass the security of their own products and services; and the systematic weakening of encryption through the mandated introduction of 'backdoors' and/or weakened standards for encryption."
[76] This is known as a 'watering hole' attack
[77] European Parliament, Directorate-General For Internal Policy, Legal Frameworks for Hacking by law Enforcement: Identification. Evaluation and Comparison of Practice (2017) at [126]
[78] BBC, NSA targeted Tor users via Firefox flaw, reports say (07 October 2013) https://www.bbc.co.uk/news/technology-24429332 <last accessed 18 March 2020>
[79] Matt Burgess, Hacking the hackers: everything you need to know about Shadow Brokers' attack on the NSA (18 April 2017) https://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers <last accessed 18 March 2020>
[80] European Parliament, Directorate-General For Internal Policy, Legal Frameworks for Hacking by law Enforcement: Identification. Evaluation and Comparison of Practice (2017)

Service (DDoS) attack against the hacktivist collective 'Anonymous'.[81] David Trail pleaded guilty to possession with intent to supply diazepam and hacking credit card details after the CPS alleged that Trail had created Topix2, another dark web marketplace. The police investigation in the UK began when the FBI handed over a range of IP addresses linked to a number of sites. It was German police that identified Trail as the controller of a dark web marketplace which had its server in Germany.[82]

The use of hacking tools in dark web cases, and in particular the jurisdictional problems that arise when applying for a warrant where the location of the device to be searched is unknown, has received much more attention in the U.S. than in other jurisdictions. This is in part because the federal nature of the U.S. brought problems relating to jurisdiction into sharp relief at an early stage and this generated a number of legal challenges concerning the point. A brief consideration of the U.S. literature before moving to look at the UK legislation governing law enforcement hacking sets out the primary problems in relation to the use of law enforcement hacking in dark web investigations. Firstly, a search is considered to take place where the suspect's computer is physically located not at the hacker's location. In 2016 an amendment to Federal Rule of Criminal Procedure 41 (rule 41) allowed a remote access warrant to be issued in a U.S. federal court despite the court being unaware of the location of the device to be searched if the device's location had been 'concealed through technological means'. The amendment was designed to allow a warrant to be issued in one federal area even though the search would potentially be executed in another. The amendment was not supposed to allow for warrants to be issued if they were to be executed outside the U.S. However, when a warrant is issued for a device with a location 'concealed through technological means' there is no way of knowing whether the warrant will be executed within the U.S. or not. In a dark web investigation, the location of the computer will not be known until after

[81] BBC news, Snowden Leaks: GCHQ 'attacked Anonymous' hackers (05 February 2014) https://www.bbc.co.uk/news/technology-26049448 <last accessed 18 March 2020>
[82] John Connell, FBI helps catch Edinburgh man selling drugs on 'dark web' (28 May 2016) https://www.edinburghnews.scotsman.com/news/crime/fbi-helps-catch-edinburgh-man-selling-drugs-dark-web-619244 <last accessed 18 March 2020>

the search is conducted. The amendment to rule 41 was specifically needed because of the expansive use of the dark web for criminal enterprise[83] and a number of high-profile rejections of warrants on the grounds of jurisdiction.[84]

In a 2017 article, Ghappour argued that the use of hacking tools by law enforcement to pursue criminal suspects who have anonymised their communications on the dark web 'presents a looming flashpoint between criminal procedure and international law'. The reason for this is said to be the fact that the 'practical realities of the technology underlying dark web investigations make it inevitable that foreign-located computers will be subject to remote 'searches' and 'seizures''[85] as there is no guarantee that the data is located within the United States. He goes on to raise issues about how such cross-border searches are authorised and deployed and suggests that 'the use of hacking tools profoundly disrupts the legal architecture on which cross-border criminal investigations rest.'[86] Benton however does not agree with Ghappour's conclusions in relation to jurisdiction. She argues that the answer to the jurisdictional conundrum is simply a further amendment to Rule 41 to specifically address the fact that a judge may issue a warrant for search and seizure of property outside of their jurisdiction as 'no other district is known to have jurisdication and the district is reasonably likely to have jurisdiction over the crime underlying the probable cause in the warrant.'[87] She argues that such an amendment would comply with constraints on extraterritorial jurisdiction and gives a list of examples as to when, in other circumstances, a state may criminalise extraterritorial conduct. The article comes to the conclusion that 'when so many aspects of criminal investigation and prosecution already reach overseas, it is

[83] Benton n (73)
[84] In re Warrant to Search a Target Comp. at Premises Unknown, 958 F. Supp. 2d 753, 761 (S.D. Tex. 2013) ("This is not to say that such a potent investigative technique [as remote access hacking] could never be authorized under Rule 41. And there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology.").
[85] Ghappour, A., Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, (2017) 69 Stanford Law Review 1075
[86] Ibid.
[87] Benton n (73)

odd that magistrate judges lack the requisite statutory authority and procedural mechanisms to issue search warrants for evidence that may be located abroad.' Such a change in the rules would not prevent LEAs from coordinating with the relevant overseas jurisdication once the foreign nature of the search is realised as a way of reducing 'conflict between sovereigns and to preserve comity'. Once a LEA learns that a computer they are searching is located overseas they:

> should cease further searching and determine whether the host nation requires further approval. At this stage sharing their investigation with host nation law enforcement agents may provide the best means of ensuring the suspect is prosecuted. Host nation authorities will have greater access to legal mechanisms to investigate the suspect, including gathering evidence on site, interviewing witnesses, and arresting the suspect.[88]

Brown agrees with this assessment also arguing that 'traditional notions of territoriality applied to physical evidence are increasingly irrelevant: when electronic evidence is involved and where a crime scene may well extend across multiple political borders'.[89]

The Investigatory Powers Act 2016 (the 2016 Act) came into force in the UK in November 2016 and aimed to formalise law enforcement use of hacking techniques and ensure greater transparency and oversight. The Act permits law enforcement to obtain data from devices by interfering with the associated electronic equipment – this provision is labelled 'equipment interference' (EI) and is set out in Part 5 of the 2016 Act.[90] The Act is accompanied by six Codes of Practice which outline the operational detail and judicial oversight arrangements which include the Equipment Interference Code.[91] The warrant must be approved by the law enforcement chief and a Judicial Commissioner[92]

---

[88] ibid

[89] Steven David Brown, 'Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice' (2020) 20 ERA Forum 423-435

[90] This capability is not new to law enforcement and would previously have been authorised as property interference.

[91]Home Office, Equipment Interference Code of Practice (March 2018) available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf <last accessed 18 March 2020>

[92] Investigatory Powers Act 2016 s. 106(1)(d)

unless the application is urgent,[93] a provision referred to as the 'double lock'. LEA's EI warrants may authorise both physical interference (e.g. covertly downloading data from a device to which physical access has been gained) and remote interference (e.g. installing a piece of software on to a device over a wired and/or wireless network in order to remotely extract information from the device).[94] LEAs may be issued with a targeted EI warrant by the appropriate Law Enforcement Chief if the warrant is necessary and proportionate.[95] A warrant can only be issued for the purposes of preventing or detecting 'serious crime'[96] or to prevent death or injury or damage to a person's physical or mental health.[97] There must be a British Islands connection meaning that at least some of the conduct, equipment interference or information must have occurred or is likely to occur in the British Islands[98] at some point.[99] Certain LEAs such as the National Crime Agency (NCA), may be issued with targeted equipment interference warrants regardless of whether there is a British Islands connection. The code of practice says that 'in practice, should a regional police force need to investigate crimes taking place where there is no British Islands connection they will do so with the assistance of another agency, such as the NCA.' A targeted equipment interference warrant can be 'thematic'[100] if it relates to multiple people, organisations or locations in the UK.[101] The Equipment Interference Code of Practice states that '[no] interference should be considered proportionate if

[93] Investigatory Powers Act 2016 s. 109 and 110. The Judicial Commissioner must still be informed the warrant has been issued and must decide within three days whether to approve the issue of the warrant.
[94] Ibid. See Chapter 3 of the code, 3.11 specifically
[95]Investigatory Powers Act 2016, s.106(1)
[96] Home Office, Equipment Interference Code of Practice (March 2016) at [4.10] This is defined as "an offence for which a person […] could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or (b) the conduct involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose" However, officers in a police force or an NCA officer colluding with a police force may also be issued with a warrant "for the purpose of preventing death or any injury or damage to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health of vulnerable individuals."
[97] Investigatory Powers Act 2016, s.106(3)
[98] "British Islands" means the United Kingdom, the Channel Islands and the Isle of Man. See Interpretation Act 1978, section 5
[99] Investigatory Powers Act 2016, s.107
[100] See Code of Practice para [5.12] "Targeted thematic warrants can cover a wide range of activity; it is entirely possible for a thematic warrant to cover a wide geographical area or involve the acquisition of a significant volume of data, provided the strict criteria of the Act are met."
[101] Investigatory Powers Act 2016 s. 101

the information which is sought could reasonably be obtained by other less intrusive means.'[102] Warrants usually last for 6 months.[103] The Investigatory Powers Commissioner's Office (IPCO) 2018 annual report notes that 'since implementation on 5 December 2018 we have seen a small number of applications to conduct EI.'[104] It goes on to accept that because of the intrusive and technically complex nature of EI it has predominantly been used by the larger LEAs and the IPCO is satisfied that the power is being used appropriately.[105] A total of 1,249 targeted equipment interference warrants were considered by a Judicial Commissioner in 2018.[106] It is not possible to know from the available statistics what proportion of these warrants were issued to LEAs.

The legislation differentiates between targeted equipment interference and bulk equipment interference.[107] Bulk equipment interference warrants are only available to the intelligence services and are approved by the Secretary of State. They are used internationally when the target or location is unknown and are used for the acquisition of communications and equipment data directly from computer equipment overseas.[108] Historically, the type of data sought may have been available during its transmission through bulk interception. The growing use of encryption has made this more difficult and, in some cases, equipment interference may be the only option for obtaining crucial intelligence. Warrants for these powers must not be sought with the intention of acquiring the communications or private data of people in the UK.[109] In such cases a targeted equipment interference warrant would be needed. The 2016 Act also creates the Investigatory Powers Commissioner and the Investigatory Powers Tribunal. The IPC[110] reviews the operation of the 2016

[102] See Code of Practice at [4.19]
[103] See Investigatory Powers Act 2016 s.117 for renewal of warrants
[104] At [11.41]
[105] Ibid
[106] Ibid at [18.4]. Note that the statistics for 2018 relate to a period of transition from authorisation under RIPA 2000 to IPA 2016 and therefore the statistics might not reflect the totality of activity
[107] Set out in chapter 3 of the Investigatory Powers Act 2016
[108] Investigatory Powers Act 2016, s. 176
[109] Such warrants were previously governed by the Intelligence Services Act 1994.
[110] Investigatory Powers Act 2016, s. 227

Act which includes all equipment interference warrants by law enforcement to ensure that the law has been complied with and fundamental rights considered; the IPT is a judicial body, independent of the government[111] which provides a right of redress for anyone who believes they have been a victim of unlawful action by a public authority using covert investigative techniques.[112] This includes law enforcement use of equipment interference.[113]

The operation of the 2016 Act in relation to warrants issued where the location of the device is concealed, as it is in many dark web cases, is opaque. On its face the Act only expressly permits hacking beyond the UK in very limited circumstances. Only bulk equipment interference warrants are specifically designed for searches overseas and they are only available to the intelligence services, not LEAs. Most LEAs[114] are required to establish a British Islands connection for an equipment interference warrant. As has been established, the nature of anonymising technology means that it must surely be difficult in some cases for law enforcement or intelligence agencies to know the physical location of the equipment they are hacking until the hacking has been conducted and the location of the target is revealed. In many dark web cases LEAs may well be unknowingly applying for a warrant to search a foreign computer. This places LEAs in a catch-22 situation. This is important as the exponential growth of the dark web means that hacking techniques are increasingly a necessary part of dark web investigations.

[111] Comprising members of the judiciary and senior members of the legal profession
[112] Provides a right to appeal from decisions and determinations of the Tribunal when there is a point of law that raises an important point of principle or practice, or where there is some other compelling reason for allowing an appeal
[113] Further information can be found at https://www.ipt-uk.com/
[114] Investigatory Powers Act 2016, s. 107. Also see Code of Practice at [3.28] "A law enforcement officer who is a member of a police force, the Ministry of Defence Police, the Police Investigations and Review Commissioner, the Independent Police Complaints Commission, the British Transport Police or the Police Services of Scotland or Northern Ireland may only be issued with a targeted equipment interference warrant is the law enforcement chief considers there is a British Islands connection.'

The Code of Conduct also has very little to say on the jurisdictional limits of equipment interference warrants. However, there are two things to note. Firstly the parameters which define when a British Islands connection exits are exceptionally wide as it includes 'any of the conduct authorised by the warrant would take place in the British Islands (regardless of the location of the equipment which would, or may be, interfered with).'[115] An example is given of an intelligence service installing a piece of software on a device located outside the British Islands by means of conduct effected within the UK. In this example a British Islands connection is said to exist because the 'conduct' i.e. the hacking, takes place in the UK.[116] Secondly, the Code states that

> to further ensure that equipment activities conducted by [specified law enforcement] agencies are focused on investigations or operations within the British Islands, irrespective of whether there is a British Islands connection, they are prohibited by the code from obtaining an equipment interference warrant for interferences that takes place outside of the British Islands unless the subject of investigation is a UK national, or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court.

The Code does recognise that other[117] LEAs, which would primarily be the National Crime Agency and the intelligence services, may be issued with targeted equipment interference warrants regardless of whether there is a British Islands connection and can therefore undertake equipment interference outside of the UK. However, should a regional police force need to investigate crimes taking place where there is no British Islands connection, according to the Code of Practice, they would do so with the assistance of the NCA. The code makes only one tangential reference to dark

[115] Code of Practice at [3.28]
[116] In addition to this a British Isles connection exists if 'any of the equipment would, or may be in the British Islands at some time' or the purpose of the interference is to obtain communications or private information relating to a person 'who is, or believed to be in the British Island.'
[117] other than those set out in section 107(2) of the Act

web investigations where an example of an investigation into a paedophile overseas struggles to name and locate the offender 'due to anonymisation'. In such a case it is said that it may be necessary for the intelligence services to examine material obtained through bulk data in order to trace victims. This would seem sensible as it is recognised that encryption makes it harder to rely on techniques aimed at intercepting a suspect's communication. Consequently, agencies need to make greater use of bulk data to identify information relating to offending.

Whilst the 2016 Act has enabled the UK to become more transparent in the granting of powers to national security and law enforcement agencies to collect, access and use data a number of issues are still unresolved and there are several issues which need to be clearer in the Codes of Practice and/or could be addressed by the IPCO. Firstly, the overlap between bulk equipment interference and thematic targeted equipment interference means that both can be used as an effective alternative to interception when encryption would render interception useless. The advent of the dark web and the need to find an alternative method of obtaining information in an age of encryption has meant that security and intelligence agencies have begun to play a vital role in supporting law enforcement to tackle the threat of serious crime. In the Government's own operational case for bulk powers it was noted that 'bulk data had supported the disruption of over 50 child sexual exploitation offenders in the UK' over a 30 months period.[118] These capabilities are particularly said to underpin the work of the Joint Operations Centre between GCHQ and law enforcement to fight child exploitation.[119] Secondly, in light of the increasing usefulness of equipment interference in dark web cases the issues that those cases present in relation to obtaining clear evidence which links an offender or their offending to the UK before a warrant is issued must be considered. As has been seen, academics have called for a fundamental rethink of

[118] UK Government, Operational Case for Bulk Powers at [3.14} available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf <last accessed on 18 March 2020>

[119] Ibid. See para [3.14} "The use of bulk data will remain essential for preventing parts of the internet from operating beyond the reach of law enforcement"

the concept of jurisdiction in relation to the collection of digital evidence and the international approach to its resolution generally and in relation to dark web investigations.[120] However despite the increasing importance of hacking tools in the investigation of serious crime brought about by the dark web neither the 2016 Act nor the Codes of Practice deals with the difficult issue of how warrants should be dealt with when the location of the computer to be searched is unknown and therefore potentially overseas.

It is suggested that, in line with legislative amendments made in other countries, the 2016 Act should be amended to clarify the position in relation to the searching of equipment in unknown locations. It should be clear to those who read the Act and its accompanying code that equipment interference warrants can be issued despite the location of the device being unknown (and therefore potentially outside of the UK) if 'the location of the device is concealed through technological means and there is evidence of a British Islands connection which justifies further investigation'. As Benton argues from a U.S. perspective,

> Federal judges should have the authority to issue warrants for the search or seizure of property under the Fourth Amendment if the alleged crime could be prosecuted in their district. This approach bridges the disconnect between courts' jurisdiction, based on physical spaces, and crimes that take place in cyberspace[121].

Such an amendment to the 2016 Act is in line with recent expanded notions of criminal jurisdiction in the field of electronic evidence.[122] It would also provide clear statutory authority for issuing warrants for places unknown and would enable the law to bridge the 'current disconnect between

---

[120] Bert-Jaap Koops and Morag Goodwin, 'Cyberspace, the cloud, and cross-border criminal investigation: The limits and possibilities of international law', Tilberg Law School Legal Studies Research Paper Series No 05/2016, available at https://ssrn.com/abstract=2698263 <last accessed on 18 March 2020>

[121] Benton n (73)

[122] Steven David Brown, 'Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice' (2020) 20 ERA Forum 423-435

territorial constraints on jurisdiction and the reality of modern cybercrime'.[123] Such an approach is needed as it is clear that the traditional approach in England and Wales of considering anything which is not illegal to be lawful is not consistent with European Convention of Human Rights jurisprudence which requires a clear legal basis for interference with a right under Article 8. It is accepted that any amendment to the law would require careful consultation which could potential begin with a review by the IPCO. The ongoing debate surrounding the legitimacy and transparency of international hacking warrants has not only been happening in the U.S. but also in Australia and in Europe.[124] A European Parliament study found that four out of six countries studied had adopted specific legislative provisions authorizing government hacking, and the remaining two were in the legislative process to enact such provisions.[125] However, of the six countries studied, only the Netherlands legally permitted the hacking of devices whose location was unknown if its location had been deliberately concealed.[126] In the Netherlands if, subsequently, a device turns out to be in another jurisdiction, Dutch police must apply for Mutual Legal Assistance to continue. If the Dutch police are aware of where the server is located, then the law enforcement authorities are required to send a request for legal assistance to the country where the server is based. If the country does not respond to the request, then the Dutch police may hack the server. The suggested amendment of the 2016 Act would align the UK with legislation in the Netherlands. Such an amendment is important for public trust[127] as well as for the effective operation of the 2016 Act. Whilst the 2016 Act has improved clarity in relation to law enforcement hacking there is still very little publicly available information on the tools that UK law enforcement agencies use, as highlighted by the following National Crime Agency (NCA)'s statement:

---

[123] Benton n. (73)

[124] Privacy International and Open Rights Group's Submission In Response To The Consultation On The Draft Equipment Interference Code Of Practice (2015)

[125]European Parliament, Directorate-General For Internal Policy, Legal Frameworks for Hacking by law Enforcement: Identification. Evaluation and Comparison of Practice (2017)

[126] Ibid

[127] For a discussion of trust in policing see Mike Hough et al., 'Procedural Justice, Trust, and Institutional Legitimacy', [2010] 4(3) Policing: A Journal of Policy and Practice 203-210

> the NCA leads the law enforcement response to serious and organised criminality impacting the UK. However, to preserve operational effectiveness we do not routinely disclose details of specific tools or techniques deployed in addressing those threats.[128]

Greater transparency as to when equipment interference can be used to hack foreign located computers does not undermine the effectiveness of such techniques nor the safety of UK citizens but would make it clear to the public that such searches are proportionate and necessary and properly overseen. The Code of Practice should also be amended to make it clear, just as the provisions in the Netherlands do, that once it is identified that a computer is located in a foreign jurisdiction mutual legal assistance channels would have to be used to further progress the investigation.

Conclusions

The Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016 have attempted to bring clarity to investigatory powers but also allowed these powers to be extended. This article has highlighted that undercover online policing and equipment interference are essential, although intrusive, police tactics in the fight against offending on the dark web. The extent to which these tactics are needed in dark web investigations is not recognised in any of the Codes of Practice related to investigatory powers and this leads to a number of problems. The 2000 and 2016 Act clarify the law but not utilisation of the law. We know what LEA powers are but not how they are used. This article has highlighted areas for potential amendment to the Codes of Practice and to the 2016 Act to ensure greater clarity and transparency. Such reform can only take place after

[128] Joseph Cox, Motherboard (26 February 2016) What the UK's Proposed Surveillance Law Means for Police Hacking https://www.vice.com/en_us/article/yp3vxb/what-the-uks-proposed-surveillance-law-means-for-police-hacking <last accessed 18 March 2020>

appropriate consultation and it is suggested this could begin by a review by the Investigatory Powers Commissioner. The following issues are specifically raised:

i) The extent to which CHIS and directed surveillance authorisations under the 2000 Act are used to authorise online covert surveillance should be publicly available. It is recommended that the IPCO annual report could break down the figures.

ii) In a time where there is a 'growth of online activity' more effort needs to be made to effectively recognise the role of online surveillance in policy documents. The ongoing Undercover Policing Inquiry is ideally placed to deal with these issues. As a minimum there should be a nationally agreed definition of an undercover online officer and Codes of Practice should recognise the key issues which arise with effective online deployment. The Codes of Practice should provide greater acknowledgment of the specific safeguards which need to be in place when conducting online undercover surveillance.

iii) The CHIS Codes of Practice or other guidance document should include discussion of the extent to which section 27 of the 2000 Act can be relied upon in undercover online operations which require an online persona to engage in activity which would otherwise be criminal, such as the posting of child exploitation material. This is particularly important in the context of CHIS and directed surveillance authorisations which only need to demonstrate that they are 'for the purpose of preventing or detecting crime' rather than the higher standard of serious crime. Whilst the 2000 Act sets out that CHIS and direct surveillance authorisations should be proportionate and necessary the Codes of Conduct give no consideration to this issue and therefore the extent to which UK LEAs engage in conduct such as that seen by Taskforce Argos in Operation Artemis is unknown and therefore lacks transparency.

iv) Jurisdiction forum shopping should not be used by any UK LEA and this needs to be explicit in the Codes of Practice. It would not be justifiable for UK police to use Taskforce Argos, or any other overseas LEA, in the way the FBI seem to have done during Operation Artemis. To deliberately seek the help of police in another jurisdiction, not because the crime had links to

that jurisdiction, but because police can use investigation tactics which are not available in the UK, would entirely circumvent investigatory powers in the UK and undoubtedly undermine confidence in UK policing. Whilst there is no evidence that any UK LEA has engaged or would engage in such conduct the current Undercover Policing inquiry has highlighted that this is a contentious area of policing which has scope to be misused and public trust is currently low. Explicit exclusion of this practice would not only help to clarify the position for LEAs but would offer an additional level of protection to defendants who wanted to challenge the practice in court. Whilst breach of the Code of Practice would not automatically result in a successful application to stay proceedings or a successful application to exclude evidence under section 78 of PACE it would likely be considered by the courts as akin to a breach of the PACE Codes of Practice.

v) The Investigatory Powers Act 2016 should address the jurisdictional issues which can arise when applying for an equipment interference warrant in dark web cases where the location of the equipment to be searched is hidden and therefore unknown. The Act could clarify that equipment interference warrants can be issued despite the location of the device being unknown (and therefore potentially outside of the UK) if "the location of the device is concealed through technological means and there is evidence of a British Islands connection which justifies further investigation". The Code of Practice should also be amended to make it clear, just as the provisions in the Netherlands do, that once it is identified that a computer is located in a foreign jurisdiction mutual legal assistance channels would have to be used to further progress the investigation.

In a 2014 report Europol called for law enforcement to build technical capabilities in order to support investigations into subjects using the dark web, in accordance with relevant legislation. The UK has responded to this call by not only increasing its capacity building and technical abilities but

also in reforming the relevant legislation.[129] It can no longer be said that the dark web is beyond the reach of LEAs in the UK and this is vital, particularly to the fight against child pornography and the expansion of illicit dark markets. Greater powers to monitor online suspects both through hacking and undercover surveillance were undoubtedly needed to ensure law enforcement can keep up with dark web offenders. This article has demonstrated that much policing of crimes committed on the dark web takes the form of traditional policing adapted for the internet and the anonymity of the dark web. Most units will spend much of their time and resources analysing open source materials, following suspicious monetary transactions and attempting to follow leads generated from arrests or interceptions of illegal packages. However, these techniques alone whilst valuable are not sufficient. Most large-scale successful take downs of child pornography forums and dark web marketplaces have utilised hacking or undercover surveillance to some extent and frequently deploy both. Historically, such covert monitoring was primarily within the domain of the intelligence agencies. The extent of offending on the dark web and the need for covert tactics to circumvent encryption has blurred the lines between intelligence agency power and police power and responsibility. As the use of the dark web by criminals expands so too will LEA reliance on investigatory powers. It is therefore more important than ever that we shine a light on this little understood corner of policing and ensure that officers have the training and legal framework required to operate effectively and the UK public can have confidence that such work is properly regulated and monitored.

[129] Although the legislation was prompted by defeats in the European Court of Human Rights