



Deposited via The University of Sheffield.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/193994/>

Version: Accepted Version

Book Section:

Purshouse, J. (2023) Citizen-led policing in the digital age and the right to respect for private life. In: Roberts, A., Purshouse, J. and Bosland, J., (eds.) Privacy, Technology, and the Criminal Process. *New Advances in Crime and Social Harm*. Routledge, pp. 92-109. ISBN: 9780367628475.

<https://doi.org/10.4324/9781003111078-5>

This is an Accepted Manuscript of a book chapter published by Routledge in Privacy, Technology, and the Criminal Process on 28 July 2023, available online:

<http://www.routledge.com/9780367628475>.

Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

Citizen-Led Policing in the Digital Age and the Right to Respect for Private Life

Joe Purshouse*

Rapid advances in technology over the course of the last decade have created opportunities for citizens to harness the power of social networking sites to engage in digital forms of ‘citizen-led policing’ (CLP), whereby citizens take a range of proactive measures to protect their communities from crime and disorder.¹ CLP initiatives have taken many forms, from more passive activities such as ‘websleuthing’² and ‘crowdsourcing’³ to ‘digital vigilantism’, which combine investigations or flagging activities that take place online with real-world confrontations with targeted individuals.⁴ The behaviours that attract the attention of CLP activists in cyberspace are equally diverse, ranging from relatively minor social transgressions and anti-social behaviour such as ‘manspreading’ on public transport to serious criminal wrongdoing.⁵

Citizens can leverage cyberspace to covertly develop relationships online; to rapidly gather evidence and disseminate information about those targeted by their crime prevention activities; to develop networks of disparate citizens across borders; and to cultivate complex working relationships with state law enforcement agencies. Such activities might previously have been considered the preserve of well-resourced state law enforcement agencies, but technological advancements and economies of scale have concentrated the power to engage in intrusive digital surveillance and other crime control-oriented pursuits into the hands of citizens. Developments in CLP could be beneficial for the authorities, reducing supply side pressure on

* Senior Lecturer in Criminal Law and Justice, School of Law, University of Sheffield. I would like to thank my co-editors and the participants in the October 2021 Seminar Series in the School of Law at the University of Sheffield for their helpful comments. All errors remain my own. I currently sit as an independent advisor to the National Police Chiefs’ Council’s working group on OCAG activity. The arguments presented here are mine alone and in no way represent the position of the Council.

¹ Katerina Hadjimatheou, ‘Citizen-led digital policing and democratic norms: The case of self-styled paedophile hunters’ (2021) 21 *Criminology & Criminal Justice* 547, 548.

² Elizabeth Yardley and others, ‘What’s the deal with “websleuthing”? News media representations of amateur detectives in networked spaces’ (2016) *CMC* 1

³ Daniel Trotter, ‘Crowdsourcing CCTV Surveillance on the Internet’ (2013) 17 *Inf. Comm. & Society* 609, 610; Johnny Nhan and others, ‘Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings’ (2017) 57 *Brit. J. of Criminology* 341 <https://doi.org/10.1093/bjc/azv118>.

⁴ Emma Hussey, Kelly Richards and John Scott, ‘Pedophile Hunters and Performing Masculinities Online’ (2021) *Deviant Behaviour* DOI: 10.1080/01639625.2021.1978278

⁵ Benjamin Loveluck, ‘The Many Shades of Digital Vigilantism. A typology of online self-justice’ (2020) 21 *Global Crime* 213, 219-220.

the finite resources of police forces, and filling any gaps in state law enforcement provision by providing the authorities with citizen-sourced evidence. Citizens can also leverage the power of the same technologies to hold state agencies and their representatives to account through planned or spontaneous acts of citizen-led journalism that mirror some of the same methods as CLP initiatives.⁶

Bespoke software applications created by multinational technology corporations are also driving innovation in CLP. In 2018, Amazon acquired smart-home security company, Ring,⁷ which soon after launched ‘Neighbors’, a free neighbourhood watch-type feature of its Ring app allowing users to upload and disseminate information about crime and safety events within a five-mile radius around their home.⁸ Since acquiring Ring, Amazon is reported to have brokered several thousand partnerships with local law enforcement agencies in the United States, which allow agencies to request access to content captured on Ring cameras.⁹ Kurwa argues that such app-based neighbourhood watch initiatives can facilitate racial profiling and produce segregationist political outcomes.¹⁰ Others have criticised platform-based community surveillance initiatives for fuelling paranoia, and encouraging citizens to mete out private retribution.¹¹ Such concerns have been compounded by developments in facial recognition technology and other forms of machine learning that could conceivably be applied to recorded content and live feeds uploaded to apps such as Neighbors, further entrenching racial biases and opening individuals up to pervasive biometric surveillance as they traverse public spaces.¹²

⁶ Bryce Clayton Newell, ‘Crossing Lenses: Policing’s New Visibility and the Role of Smartphone Journalism as a Form of Freedom-Preserving Reciprocal Surveillance’ (2014) U. ILL. J.L. Tech. & Pol’y 59, 61.

⁷ Todd Bishop, ‘Amazon completes Ring acquisition, drops price of original video doorbell under \$100’ (Geek Wire, 12 April 2018) <<https://www.geekwire.com/2018/amazon-completes-ring-acquisition-drops-price-original-video-doorbell-100/>> accessed 12 October 2021.

⁸ See Rachel Cericola, ‘Ring Neighbors Is the Best and Worst Neighborhood Watch App’ (New York Times, 3 June 2021) <https://www.nytimes.com/wirecutter/blog/ring-neighbors-app-review/> accessed 12 October 2021.

⁹ Lauren Bridges, ‘Amazon’s Ring is the largest civilian surveillance network the US has ever seen’ (Guardian, 18 May 2021) <<https://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us>> accessed 12 October 2021.

¹⁰ Rahim Kurwa, ‘Building the Digitally Gated Community: The Case of Nextdoor’ (2019) 17 *Surv. & Soc.* 111.

¹¹ See Vice News, ‘Inside Citizen App’s Dangerous Effort to Cash In on Vigilantism’ (24 June 2021) <<https://www.vice.com/en/topic/citizen>> accessed 12 October 2021; Keith Spiller and Xavier L’Hoiry, ‘Watchgroups, Surveillance, and Doing It for Themselves’ (2019) 17 *Surveillance & Society* 288, 301.

¹² Lauren Bridges, ‘Amazon’s Ring is the largest civilian surveillance network the US has ever seen’ (Guardian, 18 May 2021) <<https://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us>> accessed 12 October 2021.

Developments in CLP then are raising pressing questions concerning the appropriate role of citizens as part of the ‘web’ of surveillance and crime control provision in the digital age. A particular issue is the extent to which law can, and indeed *should*, regulate the activities of CLP activists to protect the privacy and other related rights of their targets. Through examination of the response of the UK courts to the emergence of online child abuse activism, a particular form of CLP, this paper articulates how, when citizens are policed *by* fellow citizens and not an organ of the state, the avenues for privacy protection for those targeted can be considerably narrowed. Online Child Abuse Activist Groups (OCAGs), colloquially known as ‘paedophile hunters’, are individuals or groups of individuals who pose as children on social media platforms and in online chatrooms and lure potential child sex offenders to an ostensible illicit sexual encounter. OCAGs leverage digital technology to engage in complex and intrusive forms of CLP involving surveillance and crime control. Owing to their ad hoc organisation, OCAGs operate on the periphery of the rules and norms governing state police activities. This paper argues that this situation poses an unacceptable threat to the privacy rights of those subject to their activities. It concludes that the confluence of responsabilisation of citizens in policing, technological advancement, and the hands-off approach of the lawmakers in constraining CLP activity could render laws and regulations designed to safeguard privacy from intrusive police surveillance a dead letter.

Regulating the Rise of Online Child Abuse Activists in the UK

Online child abuse activism by OCAGs has grown rapidly in the UK in recent years. There are estimated to be approximately 200 active OCAGs in the UK.¹³ OCAGs vary in terms of their composition, organisation, values, motivations, and methods. According to Crown Prosecution Service Guidance, OCAG activity can include ‘parents, who intercept a suspicious internet communication and then respond as if they are the targeted child, to sophisticated groups conducting targeted operations with an international dimension.’¹⁴ Some OCAGs engage in particularly problematic practices like live streaming face-to-face confrontations with targeted

¹³ Cahal Milmo, ‘Paedophile-hunter groups staging 100 ‘stings’ per month – and endangering law enforcement investigations, police warn’ (*i news*, 7 November 2019) <<https://inews.co.uk/news/uk/paedophile-hunter-groups-staging-100-stings-per-month-and-endangering-law-enforcement-investigations-police-warn-360294>> accessed 12 October 2021.

¹⁴ Crown Prosecution Service, ‘Online Child Abuse Activist Groups on the internet’ (23 July 2020).

individuals and even exact violent retribution, whereas others will avoid real-world confrontations and even disavow the practices of more extreme groups.¹⁵

It would be incorrect to suggest that the activities of OCAGs are free from any legal constraints. Where an activist commits a crime, he or she may be subject to criminal prosecution. Both CPS and National Police Chief Council Guidance have identified circumstances where an activist could engage in conduct that could attract criminal prosecution,¹⁶ and activists have faced charges for false imprisonment of a target,¹⁷ and blackmail.¹⁸

For OCAGs, who aim to develop usable evidence for criminal prosecutions – and state agents who may wish to rely on such evidence – the laws of evidence and procedure may also play a role in deterring unjustifiably coercive or intrusive investigatory practices. Section 78 of the Police and Criminal Evidence Act 1984 affords trial judges a discretion to exclude improperly obtained evidence if to admit the evidence would have ‘such an adverse effect on the fairness of proceedings that the court ought not to admit it.’ If an OCAG were to engage in such serious misconduct that the subsequent prosecution of a target could bring the criminal justice system into disrepute, then a court may also be permitted to stay the prosecution as an abuse of process.¹⁹

Whilst these procedural and evidential safeguards afford some protection to the fair trial rights of those targeted by OCAGs, it is doubtful they will have a material impact on either OCAG conduct or the state’s reliance on OCAG gathered evidence. Firstly, whilst state agencies will perhaps be more mindful of the risks of trials collapsing where OCAGs engage in dubious evidence gathering practices, they are also likely to understand that abuse of process doctrines and exclusionary rules offer more limited protection to defendants where those gathering the evidence for use in criminal prosecution are not agents of the state. In *R v Looseley*,²⁰ the

¹⁵ Dan Vajzovic, ‘Responding to Online Child Abuse Activists’ (NPCC, 2019).

¹⁶ Crown Prosecution Service, ‘Online Child Abuse Activist Groups on the Internet’ (23 July 2020).

¹⁷ Emily Mee, ‘Members of paedophile hunting group Predator Exposure deny false imprisonment’ (Sky News, 5 April 2019) <<https://news.sky.com/story/members-of-paedophile-hunting-group-predator-exposure-deny-false-imprisonment-11685020>> accessed 12 October 2021.

¹⁸ *R v Touzel* (Taunton Crown Court, 2 July 2018). It is noteworthy that activists may avoid criminal liability, either because of close relationships with individual officers, or lack of priority given to subtler forms of criminality. See Joe Purshouse, “Paedophile Hunters”, Criminal Procedure, and Fundamental Human Rights’ (2020) 47 JLAS 384, 394.

¹⁹ See *R v Maxwell* [2010] UKSC 48; [2011] 1 WLR 1837.

²⁰ [2001] UKHL 53; [2001] 1 WLR 2060.

leading domestic authority on entrapment, the House of Lords held that the judicial response to entrapment is based on the need to uphold the rule of law, and that this requires the courts, in each particular case, ‘to balance the need to uphold the rule of law by convicting and punishing those who committed crimes and the need to prevent *law enforcement agencies* from acting in a manner which constituted an affront to the public conscience or offended ordinary notions of fairness.’²¹ The focus for ordering a stay of proceedings, the principal remedy in cases where an individual is entrapped by the activities of an agent provocateur, is on remedying an abuse of *police* power. In *Council for the Regulation of Health Care Professionals v General Medical Council and Saluja*,²² Goldring J concluded that entrapment by a non-state agent could lead to a stay of proceedings but only in ‘very rare’ circumstances where the conduct of the non-state agent is so egregious that reliance upon it in the court’s proceedings would compromise the court’s integrity.²³

In *R v TL*,²⁴ the Court of Appeal, for the first time, considered whether a stay of proceedings for abuse of process should have been available to a defendant on the basis that he had been entrapped by an OCAG. At trial L successfully applied to stay the proceedings as an abuse of process, relying on the entrapment principles set out in *Looseley*. The Court of Appeal subsequently allowed the prosecution’s appeal. It held that the requirements of entrapment were not satisfied as the OCAG did no more than provide an unexceptional opportunity to offend and therefore the OCAG’s conduct did not come close to passing the threshold required for a stay of proceedings.²⁵ Lord Burnett CJ reaffirmed Goldring J’s observations in *Saluja* that the underlying purpose of the doctrine of abuse of process is not present in cases where the state merely relies on evidence gathered by private citizens, and that, consequently, a successful stay application in these circumstances would require particularly egregious misconduct by the private citizen. Moreover, whilst any evidence gathered using questionable or illegal investigatory practices could potentially be excluded at the discretion of a trial judge under s 78 of the Police and Criminal Evidence Act 1984, OCAGs are under no legal obligation to have regard to any relevant Codes of Practice of the 1984 Act when carrying out their investigations. This is because OCAGs are not ‘charged with the duty of investigating offences’ under s 67(9)

²¹ [2001] UKHL 53; [2001] 1 W.L.R. 2060, 2061. My emphasis.

²² [2006] EWHC 2784 (Admin); [2007] 1 WLR 3094. Henceforth ‘*Saluja*’.

²³ [2006] EWHC 2784 (Admin); [2007] 1 WLR 3094, 3110.

²⁴ [2018] EWCA Crim 1821; [2018] 1 WLR 6037 (CA).

²⁵ [2018] EWCA Crim 1821; [2018] 1 WLR 6037 (CA) [33].

of the 1984 Act, as they are not under ‘any type of legal duty, whether imposed by statute or by the common law’, to investigate offences.²⁶

Secondly, whilst in theory the existence of such safeguards may encourage OCAGs to adhere to law when conducting their sting operations, for fear that the evidence they produce will subsequently be excluded at trial, there is reason to doubt this deterrent effect. Given that many OCAGs are responding to a perceived lack of action from ‘over-regulated’ police forces and ‘leniency’ in criminal sentencing,²⁷ it is questionable whether the occasional loss of evidence or judicial admonition by the courts will have any meaningful impact on OCAGs. It is noteworthy that many of the most controversial and intrusive activities of OCAGs are not incidental to producing evidence leading to formal prosecution and trial in any way. It is safe, therefore, to assume that exclusionary rules of criminal evidence will have no deterrent effect whatsoever on common OCAG practices, such as live streaming confrontations with targets, posting addresses of family homes on the internet before charge, or degrading and berating targets.²⁸ Such activities are plainly not orientated towards the gathering of admissible criminal evidence to support successful prosecutions, and may even hamper the efforts of state agents to prosecute the targets of OCAG sting operations.

It should not come as too much of a surprise that the laws of evidence and procedure afford only tangential and minimalistic protection from intrusive OCAG activity. After all, these bodies of law are declining in significance as part of the regulatory framework that governs the conduct of police generally. Over the last thirty years, English law has adapted to developments in the police use of surveillance technology. As new surveillance technologies have emerged, they have enabled policing to become a more proactive and pre-emptive pursuit, with technologies such as automated facial recognition, DNA databasing, and even social

²⁶ *R v Bayliss* [1994] 98 Cr App R 235, 238; *R v Dhorajiwala* [2010] EWCA Crim 1237 [18]. See Purshouse, ‘“Paedophile Hunters”, Criminal Procedure, and Fundamental Human Rights’ (2020) 47 JLAS 384.

²⁷ Alidair Gillespie, ‘Paedophile Hunters: How Should the Law Respond?’ [2019] Crim LR 1016, 1019; Elizabeth Campbell, ‘Policing Paedophilia: Assembling Bodies, Spaces and Things’ (2016) 12 Crime, Media & Culture 353.

²⁸ James Hockaday, ‘Paedophile hunters snare predator and humiliate him on Facebook Live stream’ (*Metro*, 25 November 2020) <<https://metro.co.uk/2020/11/25/paedophile-hunters-snare-predator-and-humiliate-him-on-facebook-live-stream-13654092/>> accessed 12 October 2021; Alex Evans, ‘Leeds man caught in sting by paedophile hunters bringing Happy Meal to meet “12-year-old girl” for sex’ (*Yorkshire Evening Post*, 25 January 2019) <<https://www.yorkshireeveningpost.co.uk/news/crime/leeds-man-caught-sting-paedophile-hunters-bringing-happy-meal-meet-12-year-old-girl-sex-147817>>

networking sites being utilised as much as tools for obviating and deterring crime as for detecting offenders and bringing them to justice.

Whilst traditional procedural guarantees and laws governing the admissibility of evidence offer some derivative and subsidiary protection of privacy interests,²⁹ they are not designed as tools to offer prospective and encompassing regulation of pro-active, technology-led styles of policing, which focus more on the management of risky sub-populations, intelligence gathering and order maintenance than on the cultivation of admissible evidence in a criminal trial.³⁰

The growing significance of these preventive policing strategies has motivated a sea change in English law where privacy protections have become an increasingly important part of the framework regulating the coercive and intrusive activities of the police. The protections conferred by article 8 of the European Convention on Human Rights (ECHR), for example, have been subject to more expansive judicial interpretation in order to adapt to developments in the police use of new surveillance methods and technologies.³¹ Responding to these developments, a succession of regulatory statutes and secondary legislation designed to provide regulation and oversight of the police use of intrusive biometric and digital surveillance technologies have been created. English criminal lawyers have, out of necessity, had to expand their knowledge base to understand how developments in data protection law and human rights law bite on the new technologically facilitated activities and investigations of police officers. Whilst this regulatory framework is by no means beyond criticism,³² it is purported to have had a moderating effect on the shift in balance of power between the state and the individual that advances in surveillance technology have enabled.

²⁹ For example, whilst the legal principles of the right of silence, the privilege against self-incrimination, and rules governing the admissibility of improperly obtained evidence primarily operate to ensure due process and limit miscarriages of justice, they also protect privacy interests by regulating the conduct of police in searches, interviews, and other investigatory activities.

³⁰ See Satnam Choongh, *Policing as a Social Discipline* (Clarendon Press 1997); Bernard E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (University of Chicago Press 2007).

³¹ For a summary, see Council of Europe, 'Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life' (2021) 53-60.

³² See Joe Purshouse, 'Article 8 and the Retention of non-conviction DNA and Fingerprint Data in England and Wales' [2017] Crim LR 253; Nick Taylor, 'State Surveillance and the Right to Privacy' (2002) 1 *Surveillance and Society* 66; Helen Fenwick, 'Covert Surveillance under the Regulation of Investigatory Powers Act 2000, Part II' (2001) 65 *Journal of Criminal Law* 521.

To mitigate the risk of breaching privacy laws, significant tracts of operational police surveillance and investigation are now subject to senior officer-level authorisation, continuing internal and/or external oversight, impact assessments, and training requirements of individual officers. However, many of these new regulatory requirements simply do not apply to private citizens who might seek to leverage intrusive technologies to conduct their own ‘police’ work. As private citizens are increasingly able to leverage technological advances to engage in intrusive and coercive forms of crime control, there are legitimate concerns that CLP activists, such as OCAGs, will be able to circumvent privacy laws and regulations on state investigations, acting effectively as an unregulated proxy for the state, which then takes their evidence forward in formal prosecutions. The remaining sections of this analysis focus on the persistent rejection of such concerns by domestic courts, culminating in the UK Supreme Court’s (UKSC) decision of *Sutherland v Her Majesty’s Advocate (Scotland)*.³³ It will be argued that these decisions take an unjustifiably narrow, state-centric view of the scope of privacy related rights.

Narrowing the Scope of the Private Life in the Digital Sphere: The Contents-Based Approach

In *Sutherland* the UKSC dismissed the appeal of a man who argued, through counsel, that the use of communications obtained by an OCAG called Groom Resisters as evidence in a criminal prosecution was a violation of his rights under article 8 ECHR. The judgment follows a series of cases across the UK in which the admissibility of evidence gathered by OCAGs has been challenged.³⁴ In Scotland alone, 110 cases at various stages of procedure were adjourned in anticipation of this judgment.³⁵ These challenges tend to centre on whether the use of this privately gathered evidence constitutes a violation of the fundamental human rights of targets. Of central importance is the right to respect for private life under ECHR, article 8, which provides:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

³³ [2020] UKSC 32.

³⁴ See, for example, *Procurator Fiscal, Dundee v P* [2019] GWD 16 [5]; *R v TL* [2018] EWCA Crim 1821; [2018] 1 WLR 6037 (CA); *R v Walters and Ali* (Crown Court of Newcastle, 6 April 2017).

³⁵ ‘Case Comment: *Sutherland v Her Majesty’s Advocate (Scotland)* [2020] UKSC 32’ (*UKSC Blog*, 1 September 2020) <<http://uksblog.com/case-comment-sutherland-v-her-majestys-advocate-scotland-2020-uksc-32/>>.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Under s 6 of the Human Rights Act 1998 '[i]t is unlawful for a public authority to act in a way which is incompatible with a Convention right'. A prosecuting authority is a public authority for the purposes of this section, as is a court. Therefore, these bodies must, in exercising their public functions, act in such a way that is not incompatible with a Convention right such as article 8.

The facts in *Sutherland* are typical of other cases where OCAG evidence has been challenged. The Crown witness, Paul Devine, a volunteer with 'Groom Resisters Scotland', acted as a decoy. Groom Resisters Scotland provided him with photographs of a boy aged approximately 13 years old and he created an online profile on popular dating app 'Grindr'. The appellant sent sexual images and sexual written communications to Devine, acting as the 13-year-old decoy. Arrangements were subsequently made between the appellant and the decoy for them to meet in person. Activists from Groom Resisters attended the meeting place at the arranged time and confronted the appellant, broadcasting the confrontation live on Facebook. During the confrontation the police were contacted by Groom Resisters. Police officers attended during the ongoing confrontation and subsequently the appellant was prosecuted for several child sex offences. Following conviction, the High Court of Justiciary rejected an appeal which objected to the admissibility of the evidence provided by Groom Resisters Scotland on the grounds that the admission of the evidence breached his right to respect for his private life and correspondence under article 8 of the ECHR. The High Court of Justiciary referred the following compatibility issues to the Supreme Court:

1. whether, in respect of the type of communications used by the appellant and the PH group [OCAG], art 8 rights may be interfered with by their use as evidence in a public prosecution of the appellant for a relevant offence; and,

2. the extent to which the obligation on the state, to provide adequate protection for art 8 rights, is incompatible with the use by a public prosecutor of material supplied by PH groups [OCAGs] in investigating and prosecuting crime.³⁶

On the first issue, counsel for the appellant sought to argue that he held a reasonable expectation of privacy over his communications on Grindr. These were one-to-one, and so the actions of the respondent in presenting charges against the appellant based on that evidence and then relying upon it at trial interfered with his article 8 rights, notwithstanding that the conduct of the appellant was criminal. Lord Sales, with whom the other judges agreed, observed two reasons why the appellant's article 8(1) rights were not engaged. Namely, the nature of the communications from the appellant to the decoy, whom he believed to be a child, was not worthy of respect for the purposes of the application of the ECHR; and this bore on the second point that the appellant had no reasonable expectation of privacy in relation to the communications.³⁷ These reasons will be discussed in turn.

The nature of the communications. First, it was said to be implicit within the wording of article 8(1) that 'the features of his [the appellant's] private life and his correspondence for which protection is claimed under art 8(1) should be capable of respect within the scheme of values which the ECHR exists to protect and promote.'³⁸ This suggests that the protections in the qualified article 8(1) right are contingent on a value judgment by a court that the conduct of the applicant is 'capable of respect'. However, as a matter of language, the text of article 8(1) does not seem to make any such assertion. It confers a right to *respect* for private and family life, home and correspondence. The word 'respect' describes what the right holder can expect and what the corresponding duty holder must do with regard to any matter falling within, or feature of, the rights holder's private and family life, home and correspondence – subject of course to the qualifications in article 8(2). It is not implicit in the wording of article 8 that respectability is a threshold criterion of any contents of private life or correspondence for which an applicant is claiming protection.

Lord Sales also viewed the appellant's claim as inconsistent with ECHR, article 17 prohibition of the abuse of rights. The actions of the appellant were aimed at the destruction or limitation

³⁶ *Sutherland* (n 32) [11].

³⁷ *ibid* [31].

³⁸ *ibid* [33].

of the rights and freedoms of a child, and those rights and freedoms were the subject of positive obligations on the state under article 8. Accordingly, for the Court, these positive obligations outweighed any legitimate interest the appellant could have under article 8(1) to protection for his actions.³⁹ However, the appellant was not claiming that article 8 provides a right to engage in sexually explicit communications with a child. Rather, his claim was based on a violation of article 8 in its procedural sense; particularly, that the state has failed in its positive duty to all individuals, including the appellant, to provide sufficient safeguards to regulate interferences with correspondence by untrained and unvetted private citizens who circumvent laws governing state agencies before passing the evidence they gather to the police. The state has positive obligations both to prohibit and effectively deter actions aimed at the destruction or limitation of the rights and freedoms of a child *and* to ensure that adequate safeguards exist to ensure that any investigatory interferences into private life and correspondence satisfy the criteria in article 8(2). This is not affected by article 17 which is concerned solely with the actions of a group or of an individual who makes use of positive rights *for the very purpose* of destroying any of the rights and freedoms set forth in the Convention.⁴⁰

Secondly, the Supreme Court noted that the ECtHR had, in its article 8 jurisprudence, placed special responsibility on states to put in place effective deterrence measures to protect children from sexual exploitation by adults. Lord Sales cited *X and Y v Netherlands*⁴¹ and *KU v Finland*,⁴² where in the latter case the ECtHR held that:

Children and other vulnerable individuals are entitled to state protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives against activities which may pose a threat to fundamental values and essential aspects of the private lives of individuals, particularly children and other vulnerable persons.⁴³

In *KU v Finland*, an unknown person posted an advertisement of a sexual nature on an internet dating site in the name of a 12-year-old boy (the applicant), without his knowledge. The applicant became aware of the advertisement after receiving an email from a man offering to meet him. A complaint was made to the police, but the Internet Service Provider refused to disclose the identity of the person who had placed the advertisement as it considered itself

³⁹ *ibid* [43].

⁴⁰ *Lawless v Ireland* (1961) Series A no 57 [141].

⁴¹ *X and Y v Netherlands* (1985) Series A no 91.

⁴² *KU v Finland* (2009) 48 EHRR 52.

⁴³ *Sutherland* (n 32) [38]; citing *KU v Finland* (*ibid*) [46].

bound by confidentiality rules. The ECtHR held that the lack of an explicit domestic legal mechanism to compel the Internet Service Provider to divulge the advertiser's identity breached the applicant's article 8 rights. However, the ECtHR was careful to note that the state's positive obligation to provide such protection comes 'without prejudice' to the question of whether the perpetrator's conduct can attract article 8 protection.⁴⁴ Although a state has clear positive obligations to prohibit and effectively deter the sexual abuse and exploitation of children, this does not exclude from consideration that those prosecuted for such conduct must have a guarantee, albeit not absolute, that their own rights will be respected.⁴⁵ The Court in *KU* underlined:

the need to ensure that powers to control, prevent and investigate crime are exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on criminal investigations and bringing offenders to justice, including the guarantees contained in Articles 8 and 10 of the Convention, guarantees which offenders themselves can rely on.⁴⁶

Lord Sales dealt with this qualification from the ECtHR by distinguishing *KU*. Unlike in *KU*, the conduct which is made the subject of the criminal offences in the *Sutherland* was said to involve direct, sexually motivated contact 'between a paedophile and a child which is criminal in nature and is capable of affecting the child more immediately and in a more directly damaging way than the conduct in issue in *KU v Finland*.' As such, Lord Sales held that: 'the reprehensible nature of the communications is such that they do not attract protection under art 8(1).'⁴⁷

In terms of the harmfulness of the underlying conduct, it is noteworthy that, unlike taking the bait of a decoy working as part of an OCAG, the placing of the advert at issue in *KU* brought a real twelve-year-old child into direct contact with an individual who had an ostensible paedophilic sexual interest in meeting him. At paragraph 41 of its decision, the ECtHR highlighted 'the potential threat to the applicant's physical and mental welfare brought about by the impugned situation and to his vulnerability in view of his young age.' Owing to the gravity of the harmfulness of the conduct, the ECtHR rejected the Government's arguments

⁴⁴ *KU v Finland (ibid)* [49].

⁴⁵ *ibid* [49].

⁴⁶ *ibid* [48].

⁴⁷ *Sutherland* (n 32) [40].

that criminal law provisions were not needed to meet positive obligations, and yet still the ECtHR made its qualifications regarding potential continuing need to afford adequate respect to the art 8 rights of perpetrators.

To depart from this line of Strasbourg authority on the grounds that the offences giving rise to the appeal in *Sutherland* are capable of affecting the child more immediately and in a more directly damaging way than in *KU*, seems like an exercise of hair splitting rather than identifying significant differences that would warrant departure from the ECtHR approach. Lord Sales is on firm ground in suggesting that the appellant's interactions with Groom Resisters do not involve the expression of an aspect of private life which accords with the scheme of values inherent in the ECHR, but neither were the actions of the individual placing the advert in *KU*.

Reasonable expectation of privacy. In *Campbell v MGN Ltd*, Lord Nicholls observed that the reasonable expectation of privacy was a threshold standard of whether article 8 is engaged.⁴⁸ *In re JR38* affirmed that the touchstone for the engagement of article 8(1) is whether, on the facts, the individual had a reasonable expectation of privacy in relation to the subject matter of his complaint.⁴⁹ The Court in *Sutherland* followed this approach and underlined that whether a reasonable expectation of privacy exists in relation to a particular matter is an objective question. It held that the appellant could not be said to hold such an expectation with regard to his communications with the decoy.

Here, once again, Lord Sales' interpretation of the scope of article 8 sits awkwardly alongside Strasbourg authority. First, The ECtHR has consistently viewed consideration of whether an applicant had a reasonable expectation of privacy as a potential indicator of whether article 8(1) is engaged, but not necessarily a conclusive factor.⁵⁰ The UKSC also contrasted the immediate case with *Benedik v Slovenia*,⁵¹ where the ECtHR found a violation of article 8 in circumstances where the Slovenian police failed to obtain a court order before accessing subscriber information associated with a dynamic IP address as part of an investigation into the sharing of child sexual abuse material. Lord Sales observed that, whilst there may be different

⁴⁸ *Campbell v MGN Ltd* [2004] UKHL 22; [2004] 2 AC 457 [21].

⁴⁹ *In re JR38* [2015] UKSC 42; [2016] AC 1131.

⁵⁰ *PG and JH v United Kingdom* (2008) 46 EHRR 51 [57]; *Benedik v Slovenia* App no 62357/14 (ECtHR, 24 April 2018) [101]; *Bărbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017).

⁵¹ *Benedik* (*ibid*).

expectations of confidentiality in relation to use of the internet in different contexts, and even that the appellant in *Sutherland* may have enjoyed a reasonable expectation of privacy in relation to his communications for the purposes of article 8(1) so far as concerned the possibility of *police* surveillance or intrusion by the wider public, the appellant could not reasonably expect that, where his messages constituted evidence of criminal conduct on his part, the decoy as a private citizen would not pass them on to the police.⁵² In *Benedik*, the Fourth Section of the ECtHR noted that the assessment of article 8 applicability ought to be carried out ‘independently from the legal or illegal character’⁵³ of the applicant’s activity, and that the applicant’s online activity ‘engaged a high degree of anonymity’.⁵⁴ When considering whether the applicant’s article 8(1) rights were engaged a significant point of analysis for the ECtHR was whether the applicant ‘expected, from his subjective angle, that that activity would remain private and that his identity would not be disclosed’.⁵⁵

The UKSC’s reasoning takes a narrow view of the scope of article 8 protection in the context of citizen-led investigations. Lord Sales put significant weight on the criminal and potentially harmful contents of the correspondence, in determining whether article 8 was engaged. However, this approach contrasts with the ECtHR’s approach to developing the scope and normative content of article 8, which focuses on the degree to which a particular measure sets back the privacy related interests of applicants and their subjective expectations when corresponding. The ECtHR does not restrict its enquiry under article 8(1) to whether the individual can reasonably expect privacy in a particular situation, notwithstanding the fact that this may be one factor taken into consideration. This approach avoids incorporating factors that are better considered as part of an article 8(2) analysis into article 8(1).⁵⁶ In reaching its conclusion, the Court did not pay attention whether the actions of the OCAg, and the state’s reliance on the evidence they produce, were themselves compatible with the scheme of values which the ECHR exists to protect and promote by foreclosing analysis of the extent to which these were in accordance with law, and necessary in pursuit of a legitimate aim in a democratic society for the purpose of article 8(2).

⁵² *Sutherland* (n 33) [58].

⁵³ *Benedik* (n 50) [99].

⁵⁴ (*ibid*) [117].

⁵⁵ (*ibid*) [116]. See Allison M. Holmes, ‘Citizen Led Policing in the Digital Realm: Paedophile Hunters and Article 8 in the case of *Sutherland v Her Majesty’s Advocate*’ (2021) *MLR*, Early View 1.

⁵⁶ See Joe Purshouse, ‘The Reasonable Expectation of Privacy and the Criminal Suspect’ (2016) 79 *MLR* 871, 880 (note); Joe Atkinson, ‘Workplace Monitoring and the Right to Private Life at Work’ (2018) 81 *MLR* 673 (note).

Citizen Investigators and Positive Obligations to Protect Privacy

As we have seen, the UKSC in *Sutherland* found that there was no breach of article 8(1) arising from the collection of evidence by the OCAG or use of the evidence by a public authority. On the basis that article 8(1) rights were not engaged, the Court held that the state had no supervening positive obligation, arising from its duty to protect the appellant's article 8 rights, which would impede the respondent in any way in making use of the evidence about his communications with the decoy.⁵⁷ The inevitable implication of this in the immediate case was that authorisation of the OCAG by police was not required under the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) for the decoy to act as a covert human intelligence source within the meaning of that Act; and, consequently, despite no such authorisation having been obtained, the use the state of evidence gathered by the OCAG was lawful.

Whether or not it was correct in its article 8(1) analysis, the UKSC was satisfied that, in *Sutherland* and other like OCAG cases, OCAGs operate independently of the state, and so the state holds no positive obligation to regulate their conduct. This finding pre-empted the need for detailed consideration of the nature of the relationship between the state and OCAGs, and of the intrusive activity of OCAGs. The UKSC's analysis proceeded on the basis that the article 8 issue boiled down to a straight balance of the rights of the applicant to conceal his sexual communications with the decoy and the rights of potential child recipients of such communications to be free from potential harm.⁵⁸ It is not difficult to see why, when framed in this way, the balance would fall in favour of protecting the rights of potential child victims of sexual abuse over there would be perpetrators.⁵⁹

This framing overlooks the co-dependence that OCAGs have on state agencies, the potential informal relationships that have emerged between groups and state law enforcement, and the 'networked' nature of OCAG activity. The National Police Chief's Council has recently provided clarity on the strategic position of the police with regard to how officers should deal

⁵⁷*Sutherland* (n 33) [64]-[68] citing *Ribalda v Spain* (2020) 71 EHRR 7 and *SXH v Crown Prosecution Service* [2017] UKSC 30; [2017] 1 WLR 1401, with approval.

⁵⁸ *Sutherland* (*ibid*) [40].

⁵⁹ There is some academic and doctrinal support for this form of 'poetic justice' reasoning in contexts where the fundamental rights of victims and perpetrators come into direct conflict outside of a criminal process. See Tsachi Keren-Paz, 'Poetic Justice: Why Sex-Slaves Should be Allowed to Sue Ignorant Clients in Conversion' (2010) 29 *Law and Philosophy* 307.

with OCAGs. It currently endorses a position of non-proactive engagement with OCAGs, but maintains that ‘Where OCAG activity occurs we will respond positively to investigate offences and safeguard individuals involved.’⁶⁰ This goes some way to alleviating concerns that the police are working with groups on a ‘nod and a wink’ basis. However, there may be reason to question the material practical impact of the official strategic position. The same guidance document notes inconsistency at force level in responses to OCAG.⁶¹ There have also been reports of OCAGs having been offered advice by police;⁶² of prosecutions of OCAGs themselves for myriad potential offences being rare;⁶³ of the emergence in some quarters of a routine working relationship between some groups and police;⁶⁴ of police praising the work of groups;⁶⁵ and, of senior police figures speaking openly of the potential for formal collaboration with OCAGs.⁶⁶ Even though there is little evidence explicit recruiting or tasking of OCAGs by the police, there is an inevitable co-dependency between OCAGs and the police wherever the latter routinely relies on the former to build successful prosecutions. These developments raise pressing questions concerning what the true scope of the positive obligations of Contracting States should be to regulate the emergence of such ad hoc and implicit relationships between citizen and state investigators. It is unfortunate that the UKSC did not give further consideration to the appellant’s claims regarding these issues.

In *R v Walters and Ali*,⁶⁷ the question of whether implicit connections between the state and OCAGs should give rise to positive obligations on the state to authorise and regulate their activities was given more detailed consideration. The defendants in two separate cases unsuccessfully applied to stay the cases against them as an abuse of process. The gravamen of their joint submission was that it would be unfair for them to be put on trial because the evidence which would be relied upon by the Crown to justify a conviction came from OCAGs who were in effect acting as covert human intelligence sources (CHISs) but had not been

⁶⁰ Dan Vajzovic, ‘Responding to Online Child Abuse Activists’ (NPCC, 2019).

⁶¹ *ibid* at para 4.1

⁶² Purshouse (n 18); Hadjimatheou, (n 1) 556.

⁶³ Purshouse (*ibid*); Rachel McPherson, ‘Sutherland v HM Advocate: the right to privacy, evidence gathering and the integrity of justice in a digital age’ (2020) 2 Juridical Review 104, 106.

⁶⁴ Allison M. Holmes, ‘Citizen Led Policing in the Digital Realm: Paedophile Hunters and Article 8 in the case of *Sutherland v Her Majesty’s Advocate*’ (2021) MLR, Early View 1, 12.

⁶⁵ John Simpson, ‘Police praise us for job well done, say vigilante paedophile hunters’ (*The Times*, 26 April 2017) <<https://www.thetimes.co.uk/article/police-praise-us-for-job-well-done-say-vigilante-paedophile-hunters-gsjs7pjnr>> [paywall].

⁶⁶ Purshouse (n 18) 386.

⁶⁷ *R v Walters and Ali* (n 33).

subject to the degree of regulation provided for by the English version of RIPA, the Regulation of Investigatory Powers Act 2000 (RIPA).

In this case, Dark Justice, an OCAG, targeted the defendants. Each defendant interacted with a false persona, created by Dark Justice and placed on a social networking site. Each defendant was led to believe that he was interacting with a girl of 13, and, subsequently, each defendant engaged in conversations of a sexual nature and made attempts to meet the child. Langstaff J rejected the defendants' suggestion that the controls on police investigations in RIPA were unlawfully sidestepped by Dark Justice and the police, who sought to rely on their evidence.

Langstaff J first construed RIPA, Pt II and s 26 within it, as being: 'directed toward those public authorities which might use or authorise the use of a CHIS, rather than at the behaviour of an individual CHIS personally.'⁶⁸ On this view, even if Dark Justice were operating as CHISs by definition, this gave rise to no obligation on the part of the police to authorise their conduct where the police had not engaged the OCAG to act in this way. At first glance, this construction of RIPA seems to give effect to the intentions of Parliament. In the long title, RIPA makes provision for 'the use of covert human intelligence sources', not the behaviour of those who might act as a CHIS. One of the primary drivers for enacting RIPA was also to fill a lacuna in domestic law by providing a regulatory framework governing the use of covert surveillance, which meets the requirements of article 8 ECHR.⁶⁹

Langstaff J also observed that:

[T]he Act does not make the behaviour of a CHIS unlawful where it otherwise would not be so, but, rather, protects the CHIS if in the course of behaving as such he offends against the law, ... in which case any authorisation protects him against that liability. If he is not authorised to act as a CHIS, or if though authorised he is not acting within the four corners of that authorisation, he has no such protection, and is subject to any liability for which the law otherwise provides.⁷⁰

⁶⁸ *ibid* [20].

⁶⁹ RIPA was the legislative response to a number of ECtHR judgments where covert surveillance activities were held to violate art 8 because the legal basis providing for these activities was deemed insufficiently robust to be considered 'in accordance with the law' for the purposes of art 8(2) ECHR. See: *Malone v United Kingdom* (1985) 7 EHRR 14; *Govell v United Kingdom* App no 27237/95 (ECtHR, 14 January 1998); *Halford v United Kingdom* (1997) 24 EHRR 523; *Khan v United Kingdom* (2001) 31 EHRR 45; Kingsley Hyland and Clive Walker, 'Undercover policing and underwhelming laws' [2014] Crim LR 555, 560.

⁷⁰ *R v Walters and Ali* (n 33) [23].

This interpretation of the relevant provisions is persuasive and is supported by the ‘General Saving for Lawful Conduct’ provision in RIPA, s 80, which ensures that nothing in RIPA makes any action unlawful unless explicitly stated in the Act. In short, Langstaff J is saying that there is no need for the police to authorise OCAGs, where the police do not ‘use or conduct’ them, but hunters are not exempt from any liability arising from their conduct.

Much here turns on whether police have in fact ‘used or conducted’ OCAGs. In a prior article, I argued that Langstaff J adopted an unduly rigid interpretation of the phrase ‘use or conduct’ in this context.⁷¹ Langstaff J held that the police or CPS are not ‘using or conducting’ those that fall within the definition of a CHIS merely by accepting the evidence offered by them; and, they are only ‘using or conducting’ a CHIS when they specifically ask a CHIS in advance to provide information, covertly. This interpretation is inconsistent with the CHIS Code of Practice which suggests that those who, like many OCAGs, covertly gain access to personal information and voluntarily disclose this information to the police ‘on a repeated basis’ will need to be ‘managed appropriately’, and may need to be subject to CHIS authorisation.⁷² It goes further to suggest that ‘An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (ie “self-tasking”) in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes.’⁷³ Langstaff J’s interpretation of ‘using or conducting’ also seems to run contrary to a line of ECtHR jurisprudence, which indicates that where an individual had been guided and assisted by a public authority to collect evidence in a criminal case, the actions of the individual could be imputable to the public authority, thus engaging the responsibility of the state under article 8 ECHR.⁷⁴

All of this suggests that, for the purposes of the CHIS authorisation process, the question of whether the police have ‘used or conducted’ an individual to act as a CHIS under s26 of RIPA is highly context dependent. The blunt distinction drawn by Langstaff J between accepting the evidence offered by OCAGs and specifically asking an OCAG in advance to engage in covert operations and provide information to police fails to take sufficient account of the nature of the relationship that has emerged between OCAGs and the police, and its complexities.

⁷¹ J. Purshouse, (n 18) 400. Similar arguments were subsequently made in Holmes (n 63) 12.

⁷² *R v Walters and Ali* (n 34)

⁷³ Home Office, *Covert Human Intelligence Sources Code of Practice: Revised Code of Practice* (2018) [2.26].

⁷⁴ *MM v Netherlands* (2004) 39 EHRR 19 [39]; *A v France* (1994) 17 EHRR 462 [36].

As things stand, domestic law seems to afford more investigatory discretion to OCAGs than to state law enforcement agencies. Thus, OCAGs can effectively circumvent procedural safeguards and regulations that exist to moderate state power and protect the privacy rights of those subject to a criminal process. In giving unduly narrow interpretation to both the scope of article 8(1) and the CHIS authorisation provisions in RIPA and RIPA, the domestic courts have essentially left a gap in the regulation of covert surveillance undisturbed, where OCAGs can bypass the safeguards and constraints on police investigations, and prosecuting authorities can profit from the evidential fruit of OCAGs' deployment of powerful technologies and covert techniques, whilst simultaneously claiming no responsibility for its cultivation.

Conclusion

Advances in surveillance technology are driving new ways for citizens to 'get involved' in crime fighting, particularly in the digital realm. Social media has also enabled citizens to covertly develop relationships online; to disseminate information about those targeted by their crime prevention activities; to develop networks of disparate citizens across borders; and to cultivate complex working relationships with state law enforcement agencies. In the particular context of OCAG investigations in the UK, citizens can harness the power of new technologies to mimic the role of state law enforcement agencies or develop informal working relationships with them to secure criminal prosecutions, whilst bypassing legal and regulatory constraints on intrusive and coercive police practices. Citizens do not face the same level of regulation or constraint on their crime prevention activities as state law enforcement, even though they do now enjoy more power than ever before to engage in privacy-intrusive practices.

The domestic courts have taken what I have termed a contents-based approach to developing the scope and normative content of privacy rights, which focuses on the nature of communications and makes the empirical legal status of non-state actors central in assessments of whether legal constraints apply to their conduct. However, this approach is proving inadequate in the face of developments in citizen-led policing. A better approach would shift the focus towards the intrusiveness of measures used by activists and the proximity of activists in terms of their working relationships with state agencies when determining the extent to which legal constraints should apply to their conduct. To provide adequate protection to the privacy rights of those subject to citizen-led policing in the digital age, the conventional limits

of privacy rights need to be broadened, and their methodological orientation repositioned, so that the ethical and practical risks are appropriately managed.

Bibliography

— — ‘Case Comment: Sutherland v Her Majesty’s Advocate (Scotland) [2020] UKSC 32’ (UKSC Blog, 1 September 2020) <<http://ukscblog.com/case-comment-sutherland-v-her-majestys-advocate-scotland-2020-uksc-32/>>.

Atkinson J, ‘Workplace Monitoring and the Right to Private Life at Work’ (2018) 81 MLR 673 (note).

Bishop T, ‘Amazon completes Ring acquisition, drops price of original video doorbell under \$100’ (Geek Wire, 12 April 2018) <<https://www.geekwire.com/2018/amazon-completes-ring-acquisition-drops-price-original-video-doorbell-100/>> accessed 12 October 2021.

Bridges L, ‘Amazon’s Ring is the largest civilian surveillance network the US has ever seen’ (Guardian, 18 May 2021) <<https://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us>> accessed 12 October 2021.

Campbell E, ‘Policing Paedophilia: Assembling Bodies, Spaces and Things’ (2016) 12 Crime, Media & Culture 353.

Cericola R, ‘Ring Neighbors Is the Best and Worst Neighborhood Watch App’ (New York Times, 3 June 2021) <https://www.nytimes.com/wirecutter/blog/ring-neighbors-app-review/> accessed 12 October 2021.

Choongh S, *Policing as a Social Discipline* (Clarendon Press 1997).

Crown Prosecution Service, ‘Online Child Abuse Activist Groups on the internet’ (23 July 2020).

Council of Europe, ‘Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life’ (2021).

de Rond, M, Lok, J, and Marrison, A, ‘To Catch A Predator: The Lived Experience of Extreme Practices’ (2021) [online] <https://doi.org/10.5465/amj.2020.1492>.

Evans A, ‘Leeds man caught in sting by paedophile hunters bringing Happy Meal to meet “12-year-old girl” for sex’ (Yorkshire Evening Post, 25 January 2019)

<<https://www.yorkshireeveningpost.co.uk/news/crime/leeds-man-caught-sting-paedophile-hunters-bringing-happy-meal-meet-12-year-old-girl-sex-147817>>

Fenwick H, 'Covert Surveillance under the Regulation of Investigatory Powers Act 2000, Part II' (2001) 65 *Journal of Criminal Law* 521.

Gillespie A, 'Paedophile Hunters: How Should the Law Respond?' [2019] *Crim LR* 1016.

Hadjimatheou K, 'Citizen-led digital policing and democratic norms: The case of self-styled paedophile hunters' (2021) 21 *Criminol. & Crim. Just.* 547.

Harcourt BE, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (University of Chicago Press 2007).

Hockaday J, 'Paedophile hunters snare predator and humiliate him on Facebook Live stream' (Metro, 25 November 2020) <<https://metro.co.uk/2020/11/25/paedophile-hunters-snare-predator-and-humiliate-him-on-facebook-live-stream-13654092/>> accessed 12 October 2021.

Holmes A, 'Citizen Led Policing in the Digital Realm: Paedophile Hunters and Article 8 in the case of Sutherland v Her Majesty's Advocate' (2021) *MLR*, Early View 1.

Home Office, *Covert Human Intelligence Sources Code of Practice: Revised Code of Practice* (2018).

Hyland K and Walker C, 'Undercover policing and underwhelming laws' [2014] *Crim LR* 555, 560.

Hussey E, Richards K and Scott J, 'Pedophile Hunters and Performing Masculinities Online' (2021) *Deviant Behaviour* DOI: 10.1080/01639625.2021.1978278.

Keren-Paz T, 'Poetic Justice: Why Sex-Slaves Should be Allowed to Sue Ignorant Clients in Conversion' (2010) 29 *Law and Philosophy* 307.

Kurwa R, 'Building the Digitally Gated Community: The Case of Nextdoor' (2019) 17 *Surv. & Soc.* 111.

Loveluck B, 'The Many Shades of Digital Vigilantism. A typology of online self-justice' (2020) 21 *Global Crime* 213.

McPherson, R, 'Sutherland v HM Advocate: the right to privacy, evidence gathering and the integrity of justice in a digital age' (2020) 2 *Juridical Review* 104.

Mee E, 'Members of paedophile hunting group Predator Exposure deny false imprisonment' (Sky News, 5 April 2019) <<https://news.sky.com/story/members-of-paedophile-hunting-group-predator-exposure-deny-false-imprisonment-11685020>> accessed 12 October 2021.

Milmo C, 'Paedophile-hunter groups staging 100 'stings' per month – and endangering law enforcement investigations, police warn' (i news, 7 November 2019) <<https://inews.co.uk/news/uk/paedophile-hunter-groups-staging-100-stings-per-month-and-endangering-law-enforcement-investigations-police-warn-360294>> accessed 12 October 2021.

Newell BC, 'Crossing Lenses: Policing's New Visibility and the Role of Smartphone Journalism as a Form of Freedom-Preserving Reciprocal Surveillance' (2014) U. ILL. J.L. Tech. & Pol'y 59, 61.

Nhan J and others, 'Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings' (2017) 57 Brit. J. of Criminology 341.

Purshouse J, 'The Reasonable Expectation of Privacy and the Criminal Suspect' (2016) 79 MLR 871 (note).

— — 'Article 8 and the Retention of non-conviction DNA and Fingerprint Data in England and Wales' [2017] Crim LR 253.

— — "'Paedophile Hunters", Criminal Procedure, and Fundamental Human Rights' (2020) 47 JLAS 384.

Spiller K and L'Hoiry X, 'Watchgroups, Surveillance, and Doing It for Themselves' (2019) 17 Surveillance & Society 288.

Taylor N, 'State Surveillance and the Right to Privacy' (2002) 1 Surveillance and Society 66.

Trottier D, 'Crowdsourcing CCTV Surveillance on the Internet' (2013) 17 Inf. Comm. & Society 609.

Vajzovic D, 'Responding to Online Child Abuse Activists' (NPCC, 2019).

Vice News, 'Inside Citizen App's Dangerous Effort to Cash In on Vigilantism' (24 June 2021) <<https://www.vice.com/en/topic/citizen>> accessed 12 October 2021.

Yardley E and others, 'What's the deal with "websleuthing"? News media representations of amateur detectives in networked spaces' (2016) CMC 1

A v France (1994) 17 EHRR 462.
Bărbulescu v Romania App no 61496/08 (ECtHR, 5 September 2017).
Benedik v Slovenia App no 62357/14 (ECtHR, 24 April 2018).
Campbell v MGN Ltd [2004] UKHL 22; [2004] 2 AC 457.
Council for the Regulation of Health Care Professionals v General Medical Council and Saluja
 [2006] EWHC 2784 (Admin); [2007] 1 WLR 3094.
Govell v United Kingdom App no 27237/95 (ECtHR, 14 January 1998).
Halford v United Kingdom (1997) 24 EHRR 523.
In re JR38 [2015] UKSC 42; [2016] AC 1131.
Khan v United Kingdom (2001) 31 EHRR 45.
KU v Finland (2009) 48 EHRR 52.
Lawless v Ireland (1961) Series A no 57.
Malone v United Kingdom (1985) 7 EHRR 14.
MM v Netherlands (2004) 39 EHRR 19.
PG and JH v United Kingdom (2008) 46 EHRR 51.
Procurator Fiscal, Dundee v P [2019] GWD 16.
R v Bayliss [1994] 98 Cr App R 235, 238
R v Dhorajiwala [2010] EWCA Crim 1237.
R v Looseley [2001] UKHL 53; [2001] 1 WLR 2060.
R v Maxwell [2010] UKSC 48; [2011] 1 WLR 1837.
R v TL [2018] EWCA Crim 1821; [2018] 1 WLR 6037 (CA).
R v Touzel (Taunton Crown Court, 2 July 2018).
R v Walters and Ali (Crown Court of Newcastle, 6 April 2017).
Ribalda v Spain (2020) 71 EHRR 7
SXH v Crown Prosecution Service [2017] UKSC 30; [2017] 1 WLR 1401.
Sutherland v HM Advocate [2020] UKSC 32.
X and Y v Netherlands (1985) Series A no 91.

Legislation

Convention for the Protection of Human Rights and Fundamental Freedoms (European
 Convention on Human Rights)
 Human Rights Act 1998
 Police and Criminal Evidence Act 1984
 Regulation of Investigatory Powers Act 2000
 Regulation of Investigatory Powers (Scotland) Act 2000