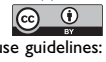
Article

The Journal of Criminal Law

The Journal of Criminal Law
2020, Vol. 84(5) 474–496



DOI: 10.1177/0022018320952560
journals.sagepub.com/home/clj

Collaborative Justice and Harm Reduction in Cyberspace: Policing Indecent Child Images

Tim J Wilson
Northumbria University Law School, UK

Abstract

The exponential increase on the internet of indecent images of children (IIOC) has been followed by a transformation within criminal justice. The scale, nature and rapid technological evolution of such crimes—often of distant initial geographical origin—requires collaborative justice and harm reduction arrangements with internet companies and NGOs. The diminished reach (declining criminal justice interventions) and power (even in identifying crimes for intervention) of state authority with the current collaborative model, however, has resulted in inadequate social regulation and policing in response to IIOC crimes on the surface web. There is a considerable risk that the *Online Harms White Paper* proposals to establish overarching government authority to generally reduce harmful conduct will not fully resolve problems that go much wider than the technological, commercial and consumer protection on the surface web issues emphasised in that document. Only political choices about funding and fundamental rights compliant legislation can (a) prevent the hollowing out of criminal justice capacity and capabilities to deal with IIOC offenders and (b) ensure an essential compatibility and consistency in police operational ability—including the access sought to anonymised communication data via an encryption key—and legal principles when dealing with IIOC crimes across all levels of the internet, including 'the dark web'. These issues are examined as a case study in civic epistemology about the influence of neoliberalism in technologically focused policy making.

Keywords

Cybercrime policing, indecent images of children (IIOC), encryption key, neoliberalism, civic epistemology

Corresponding author:
Tim J Wilson, Professor of Criminal Justice Policy, Centre for Evidence and Criminal Justice Studies, Northumbria University Law School, Newcastle upon Tyne NE1 8ST, UK.
E-mail: tim.wilson@northumbria.ac.uk

Introduction

The concept of collaborative justice appears to have originated in the USA as a description of innovative penal thinking.[1] This original usage implies: (a) *internal* initiatives (framed solely with reference to criminal justice objectives) to find external partners that can fix limitations of structure, processes and expertise (e.g. for responding to offenders' complex personal problems); and (b) that state institutions retain *agency* (absolute control over decisions to collaborate or not, and, when collaboration takes place, over its form and duration). This concept[2] provides the framework within this article for examining the extent to which cybercrime has been allowed—far beyond what was envisaged in the original US collaborative model—to be a disruptive force that reconfigures criminal justice. As such it is a case study in how neoliberal governments present policy decisions and developments that affect everyday life and reshape society—not as political choices—but as matters so determined[3] by apparently impersonal economic and technological forces that there is no alternative (often given emphasis through its expression as an acronym: TINA).[4]

The transformative potential of the neoliberal dominance over Government policy making can be seen in the significantly different collaborative justice model that has emerged for the policing or social regulation of IIOC (falling within the broader category of 'child sex abuse images', CSAIs[5]) in England and Wales. As will be seen below, it can be distinguished from the original American model by a far greater reliance on voluntary harm reduction or prevention by commercial organisations and industry funded NGOs than criminal justice interventions. Also the form and terms of the partnership with industry, especially ISPs and social media companies, and NGOs are no longer determinable solely within the public sphere. This model signifies: (a) a major retreat from a foundational concept of the state: that all actions deemed criminal under its laws are prioritised politically (in criminal justice policy) and quasi-judicially (including via prosecutorial discretion) as sufficiently grave to warrant state intervention; and (b) a change in power relationships as increasingly the state's ability to respond to certain crimes relies on often variable levels of voluntary compliance by powerful non-state partners, whose resources and political influence on technological issues may rival that of governments diminished by neoliberalism.[6]

1. For example (to quote a US website devoted to this approach): 'Court community and criminal justice professionals join forces to analyze problems and create responsive solutions; and judges, court administrators, prosecutors, defense attorneys, probation and parole representatives, corrections personnel, victim advocates, law enforcement officers, and public and private treatment providers reach out to one another to forge partnerships that will enable them to address complex medical, social, fiscal, and behavioural problems that pose significant threats to the safety and well–being of our communities'. <https://www.collaborativejustice.org/what.htm> accessed 3 January 2020.
2. The starting point is similar to Broadhurst's identification of a 'comity' of government: NGOs, industry, LEAS and academia cooperating to improve awareness of and disrupt child sexual exploitation, but the central question in this article is how such cooperation can under certain conditions transform the criminal justice system. See R Broadhurst, 'Child Sex Abuse Images and Exploitation' in R Leukfeldt and TJ Holt (eds), *The Human Factor of Cybercrime* (Routledge, London 2020) 330.
3. A parallel can be drawn with the ideological or deterministic claims about the need to embrace economic reconfiguration through 'emerging technologies with the most potential to disrupt industries and transform business models', KPMG, *The Changing Landscape of Disruptive Technologies: Tech Hubs Forging new Paths to Outpace the Competition* (KPMG International Cooperative, Zurich 2018) 1.
4. This point is also made in a general consideration of democratic accountability and policing in B Bowling, R Reiner and J Sheptycki, *The Politics of the Police* (5th edn OUP, Oxford 2019). This has wider resonance as highly centralised levers of power are increasingly manipulated on behalf of small groups of lobbyists. See C Crouch, *Post Democracy* (Polity, Cambridge 2004).
5. For example, prima facie non-erotic images of children that are used 'inappropriately' for sexual gratification are included within this term: M Yar, 'The Policing of Internet Sex Offences: Pluralised Governance Versus Hierarchies of Standing' (2013) 23 *Polic Soc* 484.
6. The 'pluralism' noted by scholars of policing has resulted in fuzzier distinctions between (a) public and private law, and social control and (b) how data sharing between public and private entities has increased the capacity for surveillance and intervention. This has resulted in moves away from state-centric policing: see Bowling et al. (n 4).

A systemic risk inherent in this model is a gradual hollowing out of capacity and capability within the criminal justice system to deal with IIOC offenders. Criminal justice interventions against IIOC crimes—equivalent to 'the tip of the iceberg' (as noted from police statements and analysed statistically in the second section) have been largely replaced by industry funded and delivered social regulation, principally in the form of disruption or image suppression. Thus the initial identification of IIOC material that—for probably the great majority of such abhorrent crimes[7]—determines whether offenders are either dealt with through the criminal justice system or allowed impunity has been vested in private entities, some of whom contribute little even to these voluntary collaborative arrangements. This demonstrates a weakening of the state's response since 2013 when Yar concluded that, in contrast to other areas of internet crime during the period studied, the policing of child abuse offences (not just IIOC, but such offences fall within and are central to his analysis) were accorded 'an unusual degree of direct intervention by state-centred authorities'.[8]

The article begins by describing two concepts—critical trust and civic epistemology—as they are used here—to understand the nature of public trust in government decision making concerned with risk management in scientifically and technologically focused policy making. The current collaboration model in which the state has yielded much of its authority over policing IIOC crimes is described in the second section. The third section seeks to unpick the reasons for signs of decline in criminal justice interventions, and the consequences of this, principally the risks arising from any hollowing-out of the criminal justice system that cannot be offset by improvements in image suppression. Technological limitations on the scope for social regulation via state-industry collaboration, notably because of the dark web (better described as anonymous communication networks: ACNs), 'going dark' in general (e.g. encryption) and relatively simple evasion (e.g. switching to a Russian ISP) are examined in the fourth section. This includes how the state's ability to respond to IIOC crimes in such environments requires matching safeguards for all its powers and activities that engage privacy and fair trial rights. The fifth section reviews two Government initiatives: the policy document, the *Online Harms White Paper,*[9] published by the May administration but still the direction of travel under Johnson, and an attempt in July 2019 to negotiate a government-industry encryption key accord. These are analysed for evidence of a fundamental break with the earlier and neoliberal influenced policies towards the role of internet companies in helping to respond to IIOC crimes. The conclusions suggest how insights from the critical trust civic epistemology concepts used in this case study can help to find a way forward on these complex and contentious issues.

Understanding Government Technologically Focused Decision Making: Critical Trust and Civic Epistemology

Walport, writing as the UK Government's then Chief Scientific Adviser, advocated critical trust as a means of addressing concerns held by lay citizens about the trustworthiness of an institution to manage scientific and technological risks:

7. Of the 105,047 IIOC URLs analysed by the IWF in 2018, 23% (24% of which were believed to be of children under two) were Category A: 'showing sexual activity between adults and children including rape or sexual torture', Internet Watch Foundation (IWF), *Once Upon a Year: the Internet Watch Foundation Annual Report 2018.* (IWF, Cambridge 2019) 18.
8. See Yar (n 5) 491.
9. DDCMS and the Home Office, *Online Harms White Paper*, (CP 57, 2019). This was published by the May administration, but legislation to implement this was indicated in the post-2019 General Election Queen's Speech (i.e. by the Johnson administration) on 19 December 2019 <https://www.gov.uk/government/speeches/queens-speech-december-2019> accessed 20 December 2019.

> Most of us have neither the time nor the expertise to examine every decision or explore all the evidence. We rely on judgements about the values and behaviours of those in charge. For the individual, 'critical trust' may be the best frame of mind: neither outright scepticism nor uncritical acceptance.[10]

This approach is important for avoiding the idea that the conferring of trust or trustworthiness is a simple binary decision (i.e. an institution is trusted or it is not).

Ward's analysis of the judicial scrutiny of the reliability of scientific expert evidence in English criminal trials, in acknowledging the relevance of critical trust alongside its limitations, offers an insight that strengthens the concept's potential analytical value: the object of critical trust is not an individual judgement or claim, but confidence in a complex system of interlocking forms of regulation and scrutiny.[11] This is not dissimilar to the scrutiny process—taking written and oral testimony from government and experts (often judiciously selected for their contrary views and opinions) in order to test government actions, policies and proposals for legislation –that Parliament uses (not always successfully) to hold the Executive to account.[12]

It is suggested here that the value of critical trust would be much greater if combined with an understanding of the fundamental ideas and assumptions the trusted themselves rely on. The origins of critical trust in a study by Walls et al. of perceptions of health and safety regulation reported that people who have only limited knowledge of the Health and Safety Executive (HSE)'s work generally trusted it to act 'altruistically' in the public interest. Significantly, they were also aware of possible limitations on the HSE's effectiveness and independence, such as lack of resources and government influence.[13] That, however, still leaves a gap in respect of 'the values and behaviours of those in charge', especially the possible prevalence of fundamental ideas and assumptions the trusted experts or institutions themselves rely on or take for granted.

In other words, are there cultural and socio-economic dispositions or group-think[14] that may restrict the range of options considered, or the seriousness with which some options are examined by decision makers? For example, the assumption in favour of 'self-regulation' or 'light regulation' [15] that proved so damaging within the finance industry may still flourish relatively unchecked as 'independent regulation'[16], or as a modified approach in which regulation is sufficient if it bears most heavily on the major entities in a market.[17] As will be seen below, these concepts that are so influential in neoliberal thinking generally about the role of government can be traced in the emergence of the problems that beset the current model of collaborative justice and harm reduction. They are also pivotal to understanding the

10. *Annual Report of the Government Chief Scientific Adviser 2015. Forensic Science and Beyond: Authenticity, Provenance and Assurance* (Government Office for Scienc, London 2015) 10.
11. T Ward, 'Explaining and Trusting Expert Evidence' (2020) 3 *International Journal of Evidence and Proof* 233–254.
12. Often scrutiny tends to result in lesser or medium degrees of policy change, unless the Government had already planned to make the recommended changes: P Lynch and R Whitaker, 'Select Committees and Brexit: Parliamentary Influence in a Divisive Policy Area' (2019) 72 *Parliam Aff* 923. This need not necessarily be so. For a comparison of the general effectiveness of Westminster scrutiny compared with Germany, The Netherlands, Nordic countries and Scotland see A King and I Crewe, *The Blunders of our Governments* (Oneworld, London 2013) 371–4.
13. J Walls, N Pidgeon, A Weyman and T Horlick-Jones, 'Critical Trust: Understanding Lay Perceptions of Health and Safety Risk Regulation' (2004) 6 *Health Risk Soc* 133.
14. For both theoretical underpinning and case studies of group think in UK government decision making, see King and Crewe (n 12) 255–67.
15. M Mazzucato, *The Value of Everything* (Penguin, London 2019) 110–34.
16. For example, D Currie, *The Currie Lecture given to the Cass Business School in London on 21 May 2014: The case for the British model of independent regulation 30 years on* <https://www.gov.uk/government/speeches/the-case-for-the-british-model-of-independent-regulation-30-years-on> accessed 29 April 2020.
17. This was the foundational idea for strengthening bank regulation after the 2008 Financial Crisis for the Basel III accord on bank capital requirements: A Tooze, *Crashed: How a Decade of Financial Crises Changed the World* (Allen Lane, London 2018) 311–4.

potential limitations of the *Online Harms* proposals and some of the risks in how encryption key access is being sought.

This approach to critical trust draws on insights from Jasanoff's studies. She conceptualises the credibility of science and technology 'in contemporary political life as a phenomenon to be explained, not to be taken for granted'[18] and equally importantly (in a different context) stresses the need to avoid 'strategic deletions and omissions'.[19] One of the strengths of her approach is that it is culturally and historically specific to the different models of democratic society in which issues are deliberated and the legal order[20] under which decisions are enacted. For example, one of her studies explains how a contentious scientific regulatory issue was resolved after an exceptionally inclusive and unorchestrated public consultation by settling on a precautionary approach. This outcome was a surprise to the UK government scientific and political establishment. They had failed, however, to anticipate the impact of a scandal that had deeply damaged public confidence in the integrity and competence in government management of health risks and scientific decision making.[21] Many examples of the risks of group-think, the subtle stifling of dissent among UK government decision makers, or only 'the survival of ideas that fit' can be found in the literature.[22] Often these have bypassed effective challenge because public understanding of other options was not encouraged, poor or constrained by the acceptance of claims that government decisions were objectively based on economic, scientific and technological knowledge that confuted alternative choices.

The 'Tip of the Iceberg': The Current Collaborative Model and Trends in Criminal Justice Interventions Against Indecent Web Images of Children (IIOC)

Senior police officers admit that the criminal justice system is only dealing with the 'tip of the [internet child abuse] iceberg'.[23] Some officers have expressed the view that the police had reached 'saturation point', and that they and the criminal justice system were 'not coping'.[24] The mirror image to such statements is that, with the exception of ANCs (anonymous communication networks or the 'Dark Web') and encrypted communications, web surveillance to find and respond to IIOC images—the 21st-century equivalent of the police beat officer patrolling the streets—is undertaken largely by commercial entities or privately funded NGOs, all of whom are currently allowed to be outside the reach of government regulation.

18. S Jasanoff, *Designs on Nature* (PUP, Princetown 2005) 250 and 255.
19. S Jasanoff, 'The Idiom of Co-production' in S Jasanoff (ed), *States of Knowledge* (Routledge, Abingdon 2006) 3.
20. 'An aggregate or a plurality of general and individual norms that govern human behavior, . . . [comprising] legislative acts, acts constituting legally binding custom, judicial acts, administrative acts, and private law transactions, in particular contracts': H Kelsen, 'The Concept of the Legal Order' (tr SL Paulson, 1982) 27 *American Journal of Jurisprudence* 64–65. An outstanding example of the value of Jasanoff's approach is her comparative study of the development of embryology regulation and biotechnology patent law in the UK, Germany and the USA, Jasanoff (n 18) 146–224.
21. The scandal was the cattle disease, BSE, and the contentious scientific regulatory issue was GM food: Jasanoff (n 18) 256–8, 121–30.
22. A much earlier example is the selection of gas cooled reactors in the 1960s: J Kay, *The Truth About Markets* (Penguin, London 2004) 91–93 and a later example is Prime Minister Thatcher's ill-fated Poll Tax (collected in England and Wales in 1990–93): King and Crewe (n 12) 41–63, 256–7 (group-think); 335–337 (ignoring a realistic alternative); and, more recently: A Stevens, 'Governments cannot just "follow the science" on COVID-19' (2020) *Nat Hum Behav* < DOI: https://doi.org/10.1038/s41562-020-0894-x > accessed 27 May 2020.
23. Noted—in the context of on-line abuse—during field work (subject to the Chatham House Rule), for example, at a NPCC sponsored conference held on 19–21 November 2019. The same phrase, irrespective of internet involvement, is also used about offences against children generally: Home Affairs Committee, *Policing for the Future* (HC 2017–19, 10) para 80.
24. Independent Inquiry into Child Sexual Abuse (IICSA), *Investigation Report: The Internet* (HMSO, Richmond 2020) para 60.

The Government frequently draws on information provided by this global community when describing the scale of IIOC offending. An important UK Government 2020 publication[25] cited 16.8 million referrals in 2019 to the US National Center for Missing and Exploited Children (NCMEC) to illustrate the scale of internet abuse. When doing so it failed to indicate that this figure was a global total, a significant proportion of the material may have no UK connections and to acknowledge that such data includes virtual child pornography (VCP),[26] imagination based images, such as cartoons and drawings,[27] self-generated IIOC images ('youth sexting') or, possibly prima facie non-erotic images that may have had an innocent origin. Such statements, while reflecting important successes in responding to IIOC crimes, focus on the symptoms and not the causes or direct risks of such offending.

Any account focused on the direct UK causes and risks of IIOC crimes needs to start with an estimate that this country's residents are 'the third-largest global consumers of internet child abuse images'[28]—a group of possibly 80,000 individuals[29]—and the inestimable number of children they harm. If these estimates are reliable, this level of potential criminality is a daunting initial surveillance challenge for the police. It is approximately on the same scale as US internet surveillance or espionage against foreign data subjects revealed by Snowdon, and only about 30,000 short of the number of 'new entrants' to the criminal justice system in England and Wales (many for minor and easily dealt with offences e.g. TV licence evasion) in the year ending December 2018. [30] Finding ways to reach this group of IIOC offenders and responding to them as individuals has to be a principle objective of criminal justice policy relating to web IIOC images and must not be confused with the equally important but offender and victim remote policy objective: image suppression.

As far as circulated images are concerned, ISPs (Internet Service Providers) and other digital industry entities have created powerful disruption apparatus. In 2018 the industry-funded IWF (Internet Watch Foundation)[31] ensured that 29,865 UK hosted posts were suppressed or 'taken-down' quickly (45% within two hours). This appears to have made the UK surface web a comparatively hostile environment for IIOC commerce. This country's estimated share of the global total of hosted child sexual abuse content is believed to have fallen from 18% in 1996 when the IWF was established to 0.04% in 2018.[32] Since 2018 the IWF has been given accessed images collected during police investigations and recorded on the UK police Child Abuse Database (CAID). The IWF distributes new CAID images to IWF industry members so that any copies accessible elsewhere through services controlled by its members can be deleted.[33] At first sight, these results suggest that this collaborative model—based primarily on self–regulation and measured in terms of image suppression, not, as will be seen below, criminal justice interventions—is a pragmatic response to technologically determined

25. DDCMS and Home Office, *Online Harms White Paper—Initial consultation response* (DDCMS and Home Office, London 2020) 1.
26. Theoretically computer generate images, but not a straightforward category: AA Gillespie, *Cybercrime* (Routledge, Abingdon 2019) 249–54.
27. Broadhurst (n 2) 315.
28. Behind the USA and Canada: Home Affairs Committee (n 23) para 83.
29. IICSA, *Investigation Report: Children Outside the United Kingdom Phase 2* (HMSO, Richmond 2020) 1.
30. 89,138 NSA surveillance targets in 2013: D Lindsay, 'The Role of Proportionality in Assessing Trans-Atlantic Flows of Personal Data' in DJB Svantesson and D Kloza (eds) *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (Intersentia, Cambridge 2017) 60. 107,174 new entrants: ONS, 'Offending History Data Tool: First Time Entrants Statistics' *Criminal Justice System statistics quarterly: December 2018*, <https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2018> accessed 16 December 2019.
31. In 2017/18 its income of approximately £3million came primarily from industry subscriptions (£2.3miilion; industry representatives on its board are drawn from major donors, Google, Microsoft and Virgin Media). It also received a £0.4 M in EU grant. *Internet Watch Foundation Trustees' Report & Financial Statements For the year ended 31 March 2018* (IWF, Cambridge 2018).
32. IWF (n 7) 27, 35 and 45.
33. IWF, *IWF connects to the Child Abuse Image Database (CAID)*, 21 March 2018 <https://www.iwf.org.uk/news/iwf-connects-to-child-abuse-image-database-caid> accessed 25 October 2019.

change in the nature of crime. In line with neoliberal thinking it also limits the role of the state and avoids significant public expenditure.

The Government, the IICA (the Independent Inquiry into Child Sexual Abuse), and in the USA, the NCMEC (see the last two sections), however, have called for significant reforms to the present collaborative model so that businesses within regulatory reach cannot evade, for commercial reasons, their responsibilities to take action against child abuse by their service users. This reflects a significant change in Government thinking compared with 2017, when a Parliamentary inquiry looking at wider questions relating to children and internet safety identified a neoliberal preference for industry self-regulation.[34] From a criminal justice perspective, the current commercially led arrangements, possibly combined with the Government's somewhat undisciplined emphasis on the scale of global IIOC image data, also have unanticipated adverse consequences. For example, the greater unfairness (almost akin to 'entrapment') risk when evidence is gathered by 'paedophile hunters', who believe their activities fill a void left by the police.[35]

The National Crime Agency (NCA) received from industry sources 113,948 reports of child sexual abuse material believed to be UK-related in 2018.[36] It is impossible to be certain how this statistic compares with three million images a year being added to CAID in 2019 from devices seized by the police.[37] If, however, the CAID volume is compared to the 2019 estimated 6,000 IIOC arrests annually,[38] the number of images for every arrest would average 500. That would be a comparatively low number given the scale of material seized from individuals in some investigations.[39]

There is a considerable volume of evidence to be assessed when taking cases to court, but the potential burden of work after an arrest has to be seen in context:

- There are few defences to the main IIIOC offences relating to making or possessing etc. IIOC images: s 1 of the Protection of Children Act 1978 or s 160 of the Criminal Justice Act 1988. They are restricted to law enforcement, national security or within marriage.[40]
- It is estimated that every single mobile device examined by the police can contain an average of 35,000 pages of data that can be downloaded.[41] For most crimes, especially in rape investigations, the search for relevant and admissible digital evidence or identifying disclosable material will be more difficult and time consuming than dealing with the evidence needed to satisfy liability for IIOC crimes.

34. Communications Committee, *Growing up with the internet* (HL 2016–17, 130).
35. Entrapment is not a defence in English law, but the courts may intervene on grounds of unfairness: AA Gillespie '"Paedophile Hunters": How should the Law Respond?' (2019) 12 *Crim LR* 1016-1034; Brants et al. 'A comparative Analysis of Anglo-Dutch approaches to "cyber policing": checks and balances fit for purpose? and Davies 'Shining a Light on Policing the Dark Web: An analysis of UK investigatory powers' in this issue.
36. NSPCC, *How Safe are our Children? 2019 Online Abuse An Overview of Data on Child Abuse Online* (NSPCC, London 2019) 24.
37. S Preston, 'New AI Technology to Safeguard Children & Catch More Predators', *Safeguarding News* (19 July 2019) <https://ssscpd.co.uk/news/safeguarding-e-bulletin-18th-july-2019> accessed 3 February 2020.
38. IICSA puts the figure at 'approximately 400–450', but that figure was given to inquiry in May 2019, IICSA (n 24) 2.4. The figure quoted here reflects police officer reports of an 'average 500 or so each month' at Chatham House Rule events organised by City Forum on 24 October 2019 and the NPCC on 19–21 November 2019.
39. Noted at random, *R v Adam Magness* [2019] EWCA Crim 2071 involved a case of four charges under s 1 PCA 1978 and s 160 CJA 1988 that related to over 27,000 images and 150 'movies'.
40. The exemptions are more easily traced in *Archbold: Magistrates Court Criminal Practice* (11th edn Sweet and Maxwell, London 2015) 14–62 to 14–63, 14–67 to 14–69.
41. V Baird, *Written evidence from Office of the Police and Crime Commissioner for Northumbria* (DIS0025) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80665.html> accessed 3 February 2020.

Almost £20 million has been invested in CAID infrastructure, including in 2019 £1.76 million to fund 'game-changing' innovations to CAID to speed up investigations.[42]

Each newly discovered IIOC image can be given a unique signature (or 'fingerprint'/'hash') by using Microsoft's PhotoDNA to identify 'first generation' images, thus avoiding duplicate recording when an image has already been placed on a networked criminal justice or NGO database.[43]

The above points are not made to downplay the demands created by criminal justice interventions resulting in 22,896 obscene publications offences recorded in England and Wales (the NSPCC suggest that 94% related to images of children) during 2017/18,[44] particularly, as will be considered later, when making difficult decisions (often involving complex psychological and risk assessments[45]) about arrested and convicted offenders. The impact of IIOC offences on criminal justice workloads, however, should be seen in the context of the exponential rise and additional complexity of both cybercrime (including online monetary offences and illicit trading) and digital evidence for a much wider range of offences.[46] The overall impact of these digital and cyber trends, including IIOC offences, is not just seen in the UK, as 'a threat to [police] capability to investigate such crimes and identify victims'.[47]

Table 1. IIOC and sexual grooming offence statistics 2017 and 2018 (on an all offences charged basis).[48]

Home Office Offence Code **(n.b. also the key to HO codes in Figures 1-3 below)**	2017 Principal offence Prosecution/ Conviction ratio	2018 Principal offence Prosecution/ Conviction ratio	2017 Non-principal offence Prosecution/ Conviction ratio	2018 Non-principal offence Prosecution/ Conviction ratio
86.1 (creation, publication and distribution of indecent child images)	3,132/3,020 (96.4%)	2,298/2,193 (95.4%)	8,839/8,817 (99.8%)	6,155/6,086 (98.9%)
86.2 (possession of indecent child images)	339/385 (113.6%)	235/248 (105.5%)	1,726/1,633 (94.6%)	1,057/1,041 (98.5%)
86.3 (possession of prohibited child images)	29/47 (162.1%)	29/35 (120.7%)	749/674 (90.0%)	626/550 (87.9%)
88A ('Sexual grooming' of a child)	330/241 (73.0%)	441/359 (81.4%)	522/216 (41.4%)	1,027/350 (34.1%)

The most detailed statistics (counting offences not defendants) about criminal justice interventions are summarised below in Table 1. The prosecution to conviction ratios, when expressed as percentages,

42. For example, the analysis of 1 TB drive content to identify IIIOC images should take 30 minutes, when previously it would take up to 24 hours, and 2,000 images an hour should be graded for severity (prior to human inspection) compared 200 if manually graded, Preston, (n 37).
43. 'A child sexual abuse image taken by an adult that has not previously been recorded by law enforcement or industry as indecent': IICSA (n 24) 111. For PhotoDNA see: ECPAT, *Internet and Technology Fact Sheet: What are Hashes? What is Photo DNA?* <https://www.ecpat.org/wp-content/uploads/2016/04/IT%20Factsheet%20-%20What%20is%20PhotoDNA_0.pdf> accessed 12 December 2019.
44. NSPCC, (n 36) 23–24. (There were an additional 658 offences in Scotland and 478 in Northern Ireland.)
45. In addition to the issues considered in the next section, the author, when listening to police officers discussing their work, noted their concern about arrestee suicide risks.
46. For example, see: BBC News, 'Problems with Disclosure Resulted in the High-profile Collapse of a Number of Prosecutions for Rape Cases between December 2017 and spring 2018 or in convictions being quashed. MPs criticise head of public prosecution's criminal case failures' (20 July 2018) <https://www.bbc.com/news/uk-44892607> accessed 3 February 2020.
47. Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (Europol, The Hague 2018) 31.
48. ONS (n 30), 'Experimental Statistics: All offences by Home Office Code'.

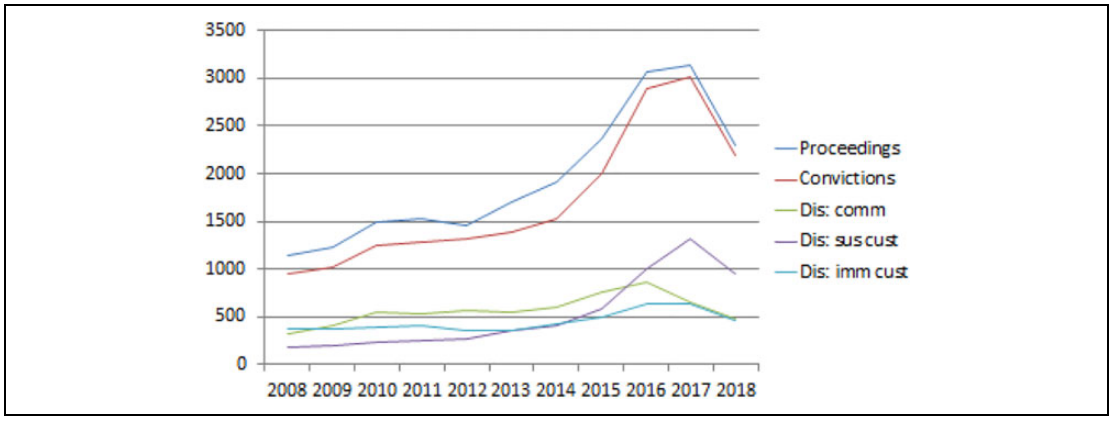


Figure 1. Outcomes on a principal disposal basis—HO Code 86.1.

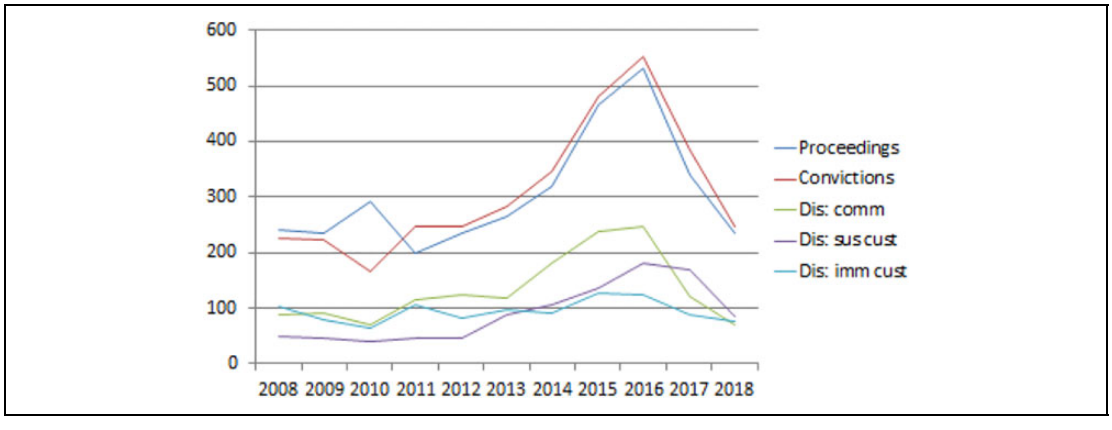


Figure 2. Outcomes on a principal disposal basis—HO Code 86.2.

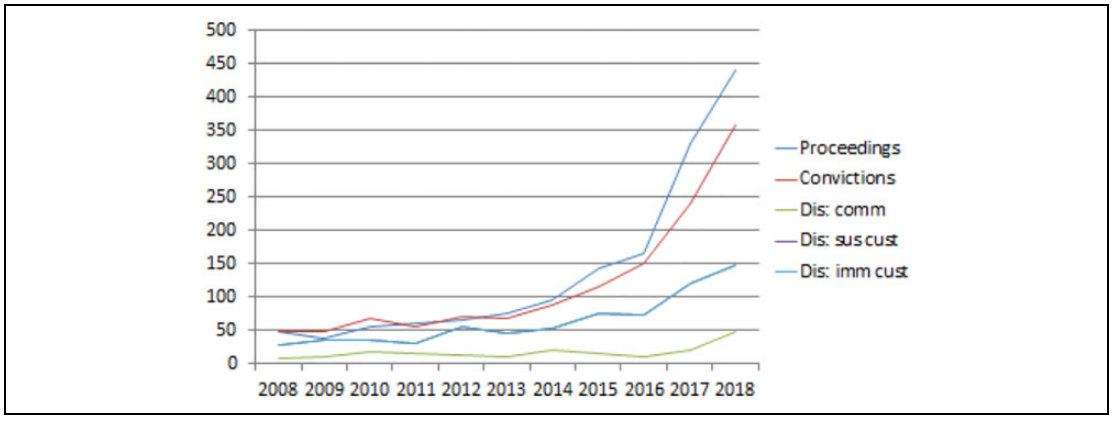


Figure 3. Outcomes on principal disposal basis—HO Code 88A.

by showing figures in excess of 100% suggest a reduced flow of new offences prosecuted each year compared with proceedings completed during that period measurable as convictions.

This downward trend in criminal justice interventions against IIOC offences can be seen more clearly in the standard criminal statistics summarised in Figures 1 and 2 below, with a comparison with the markedly different pattern for child sexual grooming at Figure 3 (for the key to the HO codes see Table 1). [49] Unlike the data summarised in Table 1, these only provide information about the offence that attracted the most severe sentence or outcome (the principal disposal basis). The volume of IIOC proceedings doubled between 2013 and 2016 but then fell significantly. While these lack the detail of the statistics analysed in Table 1, the picture presented by the principal disposal data is also consistent with the view that 'the tip of the iceberg' may well be getting smaller.

The decline in IIOC criminal justice interventions contrasts markedly with the impression given by police estimates of a national increase in IIOC offences of 424% between 2013–14 and 2017–18[50] and an increase in IWF recorded 'child sexual abuse URLs' by 54% between 2015 and 2018.[51] The decline in IIOC proceedings also appears to be greater than general criminal justice trends, for example, the aggregate 12% reduction in the number of arrests nationally between 2016 and 2017.[52] With the exception of grooming, the statistics demonstrate a significant contrast with Yar's conclusion in 2013 (consistent with the above data analysis at that time) that, in contrast to other internet crime, the policing of child abuse offences were accorded 'an unusual degree of direct intervention by state-centred authorities'.[53] It has be assumed that the reasons for the decline in criminal justice interventions are likely to be attributable to policy choices, including resource allocation decisions, not changes in criminal behaviour.

Unpicking the Reasons for the Decline in Criminal Justice Interventions and the Potential Consequences

The political and economic circumstances that gave rise to the current collaborative model and intimations of the risk that—despite the impression created by *Online Harms*—statutory regulation might not result in fundamental reform are partly explained by Zuboff's analysis of 'surveillance capitalism': a concentration of monopolistic capitalism that confers democratically unaccountable and transnational political power derived from the concentrated ownership of data analysis and communication platforms. She notes the significance of 'the neoliberal capture of the government machinery for oversight and regulation of the US economy'[54] for how this developed during the decades that bridged the Millennium, particularly how the relationship between right-wing politics (neoliberal and libertarian) and the nascent power of Silicon Valley blocked attempted US government oversight of abusive content on the web.[55]

This section focuses on aspects and consequences of the neoliberal dominance over policy making that (a) go beyond Zuboff's analysis and (b) are criminal justice specific: the reasons for the downward statistical trends and how, if this is a sign of the hollowing-out of capacity and capability within the criminal justice system for dealing with IIOC crimes, this could result in risks that cannot be offset by improvements in image suppression.

49. ONS (n 30), 'Outcomes by Offence Data Tool (Criminal Justice System Statistics publication: Outcomes by Offence 2008 to 2018: Pivot Table Analytical Tool for England and Wales—Time Period: 12 months ending December 2008 to 12 months ending December 2018'. (The 2019 data was not available when this article was submitted for publication.)
50. Home Affairs Committee (n 23) para 84.
51. IWF (n 7) 19.
52. ACRO Criminal Records Office, *Annual Report 2017-2018* (ACRO, Southampton 2018) 11.
53. Yar (n 5) 491.
54. S Zuboff, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (Profile Books, London 2019) 107, 37–46.
55. Ibid 107–112.

Inadequate capacity is not a uniquely English problem. This is clear from NCMEC testimony (March 2020) to the US Senate Judiciary Committee:

> Relatively static governmental funding to address the horrifying increase in child sexual exploitation content being circulated worldwide has become an impediment in effectively combatting this problem.[56]

The Metropolitan Police have acknowledged that criminal justice internet child abuse interventions have been limited by pressures arising from other contemporary priorities, especially anti-terrorist activities that pose immediate and severe risks, and fiscal austerity.[57] A Parliamentary report has noted frequently reported backlogs in 'digital evidence' work. [58] Fiscal austerity has had an adverse impact on both the number of police investigators and the availability of forensic science and technology support.[59] Presumably some police child abuse specialists working on IIOC crimes since 2014 have also been redirected to important investigation of an ever increasing number of historic sexual abuse allegations.[60] Such diversion may only be temporary, but it serves as a reminder that any loss of police IIOC investigation capacity because of policies premised on the view that industry managed image suppression is sufficient, is likely to damage the ability to swiftly redeploy some of the staff with expertise in crimes against children to investigate other forms of child abuse.

Other problems stem from inadequate police resources, including the likelihood that criminal justice interventions would increasingly reflect UK-centric prioritisation. The Philippines is the greatest source of IIOC material,[61] whereas sexual grooming—where criminal justice interventions continue to rise—will normally take place in-country. Such policy choices would be consistent with IICA commissioned research findings about restrictions on known offenders. Only 0.2% of sexual harm prevention orders imposed in 2017/18 included foreign travel restrictions. The Commission questioned this introspective approach to child protection. They recommended international intelligence sharing similar to that for money laundering so that travel restrictions could be targeted proportionately to prevent travel to destinations notorious for child abuse.[62] This recognition of the importance of proportionality also serves to emphasise that Government policy and police operational priorities cannot just focus on supressing abuse images. Criminal justice casework tailored to the circumstances and risks of individual offenders, harm suffered by victims and potential future risks of either offending or harm needs to be adequately funded.

IIOC offences were not within the remit of the Law Commission's 2018 scoping study of abusive and offensive communications,[63] but what it stated about the significance of the criminal law in the different context of its work on online offences is arguably also applicable to web IIOC crimes:

> While the challenge of addressing the scale and reach of abusive and offensive online communications may seem overwhelming, we consider that the law, and in this particular context the criminal law, has an important role to play in punishing and deterring the most serious conduct, and in shaping community attitudes as to its unacceptability.[64]

In a similar tenor the Home Office acknowledged to the IICA—when reporting that diversion strategies had proved to be more resource-intensive than prosecution and risk management assessments had been

56. J Shehan, Exploited Children Division, NCMEC, *Testimony to the Senate Committee on the Judiciary* (11 March 2020) 5.
57. IICSA (n 24) para 62.4.
58. Home Affairs Committee (n 23) para 88.
59. TJ Wilson, 'The Impact of Brexit on the Future of UK Forensic Science and Technology' (2019) 302 *Forensic Sci Int* 5.
60. V Dodd, 'Police Uncover "Epidemic" of Child Abuse from1970 s and 80s', *The Guardian* (6 February 2020) 1–2.
61. Europol (n 47) 35.
62. IICSA (n 29) 54–55.
63. I Law Commission, *Abusive and Offensive Online Communications: A Scoping Report* (Law Com No 381, 2018) para 6.1.
64. Ibid para 13.3.

found to be problematic—that there is a 'need for justice to be served in terms of victim impact' by ensuring that a conviction is recorded.[65]

Criminal proceedings are distinguishable from social control or aggregate contributions to social welfare because of a unique retributive function in which due process is integral with the objective of 'blaming wrongdoers according to their just deserts'.[66] Retributive justice should not, however, be confused with narrow punitiveness, especially bearing in mind that imprisonment often does more harm than good. Criminal justice interventions must be proportionate to the degree of and responsibility for harm: for example, in the IIOC context, between primary harm, where an image was produced through child rape and secondary harm arising from a victim's recurrent anxiety about the continued circulation of a partly naked image.[67] Prosecutors and judges are not only capable of dealing with such potentially complex matters, but the fact that their decisions, and the rules or guidelines under which they are made are open to scrutiny is vital for maintaining critical trust in the criminal justice response to internet IIOC crimes.

An emphasis on focusing on image suppression over criminal justice interventions against individuals acquiring IIOC images also means numerous lost opportunities to encourage desistence (even if this may rely more for success on activities and influence outside the criminal justice system, the criminal justice intervention may be needed to initiate behavioural change) and, at a minimum, bring the individuals within sex offender risk management arrangements.

It is unclear whether significant numbers of passive consumers of IIOC images are likely or not to become contact offenders (e.g. shift their offending to sexual grooming and beyond). Research in this area is relatively new and the results are inconsistent, but generally studies suggest that the internet has a disinhibiting effect that facilitates offending behaviour.[68] There is a significant risk that consuming sexualised imagery of minors and sexually abusing minors 'may exist in a mutually enforcing dynamic'.[69] Police views and IIAC commissioned assessments suggest that between 16% and 50% of child abuse cyber criminals will later commit physical offences, [70] fewer criminal justice interventions certainly means that more potentially dangerous offenders will remain unknown to the police and thus evade child safeguarding measures.

This safeguarding system was created to protect children and vulnerable adults following the Soham child murders in 2002. Adoptive parents, salaried workers and volunteers are vetted for evidence of criminal behaviour that could indicate a risk of harm if there is future regular contact with children.[71] Under these arrangements persons convicted or cautioned for an offence, inter alia, under s 1 of the 1978 act or s 160 of the 1988 Act are automatically barred from such activities and roles.[72] The police also have discretion to reveal information about an IIOC incident to a potential employer etc. for safeguarding purposes, even if proceedings were not initiated. The exercise of discretion has to be proportionate and, as a process undertaken by a public authority, the decision making process can be challenged through judicial review.

As noted earlier, the potential complexity of criminal justice casework decisions relating to IIOC is reduced by the limited defences to possession etc. under s 1 PCA 1978 or s 160 CJA 1988. There is a downside to this that is relevant to the advantages and, in some respects, the need for the response to IIOC images to remain in the hands of adequately resourced and publicly accountable agencies. When

65. ICSA (n 24) 42.
66. P Roberts and A Zuckerman, *Criminal Evidence* (2nd edn Oxford University Press, Oxford 2010) 11.
67. For a discussion of primary and secondary harm, see Gillespie (n 26) 231–6.
68. Broadhurst (n 2) 317–9.
69. Yar (n 5) 485.
70. Home Affairs Committee (n 23) para 85.
71. ACRO (n 52) 43.
72. Disclosure and Barring Service (DBS), *Factsheet 5: Relevant Offences* <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/157242/dbs-factsheet-05.pdf> accessed 14 January 2020. There are limited grounds to appeal DBS decisions under the Safeguarding Vulnerable Groups Act 2006.

these statutes were enacted, Parliament could not have anticipated self-generated imaging (SGI, or 'youth sexting'). To avoid wrongly criminalising young people the police were encouraged in 2015 not to initiate proceedings in certain circumstances: where the making and sharing of the image is 'non-abusive and there is no evidence of exploitation, grooming, profit motive, malicious intent (e.g. extensive or inappropriate sharing . . .) or . . . persistent behaviour'. The police were also advised to exercise discretion in disclosing information about such an incident, should the young person responsible later apply for a safeguarding check.[73]

This issue also might cast further light on the downward statistical trends. FOI data obtained by *The Guardian* suggests that as a result of the 2015 guidance only 0.5% of SGIs incidents involving children under 14 over almost 34 months up to August 2019 resulted in a charge, caution or court proceedings.[74] With 241 SGI under 14 investigations a month, this change in policy could have had a significant impact on the IIOC intervention statistics with a total of 500 child abuse arrests each month according to the police (2019)[75] and the Government (2020)[76] There is certainly a temporal correlation between the publication of the 2015 guidance and the emergence of downward trends, particularly when allowance is made for the initially inconsistent application of the guidance by different police forces.[77]

Sexting is a risky behaviour, but Gillespie (writing prior to the 2015 guidance) suggested that the alternative to adolescent criminalisation was:

> A more proportionate approach would be to recognise this harm by requiring the identification and prosecution of the individual who distributes the images more widely, including to the Internet at large.[78]

This begins to reach the heart of the government policy inconsistency in the current collaborative arrangements. This can be seen more clearly in the different treatment of adults as individual citizens compared with the laissez faire approach to industry, either corporate entities or their senior executives. In 2019 a senior police officer, Supt. Williams, received unsolicited (it seems from newspaper reports not to have been disputed) IIOC images on her phone and alone among 15 other recipients of these images was prosecuted.[79] In contrast to this, ISPs and the providers of platforms to which photographs can be uploaded and then generally accessed—including 'revenge' sites' - enjoy impunity from any culpability for IIOC offences in England and Wales, indicated in a Government statement:

> The prohibition of content on the Internet, that is potentially illegal under this law by British internet service providers, is however self-regulatory, coordinated by the non-profit charity Internet Watch Foundation (who has partnerships with many major ISPs in the country). The IWF operates in informal partnership with the police, government, public and Internet service providers.[80]

---

73. Known as 'Outcome 21 Guidance ', College of Policing, *Briefing Note: Police Action in Response to Youth Produced Sexual Imagery ('Sexting')* (College of Policing, Ryton 2016) 5.
74. J Halliday, 'Alarm as Over 6,000 Children are Investigated by Police for "Sexting"' *The Guardian* (31 December 2019) 9.
75. IICSA (n 24) 2.4 puts the figure at 'approximately 400–450', but that figure was given to inquiry in May 2019. The figure used here reflects police officer reports of an 'average 500 or so each month' at Chatham House Rule events organised by City Forum on 24 October 2019 and the NPCC on 19–21 November 2019.
76. DDCMS and Home Office (n 9) 1.
77. E Bond and A Phippen, *Police Response to Youth Offending Around the Generation and Distribution of Indecent Images of Children and its Implications* (University of Suffolk and the Marie Collins Foundation, Ipswich 2019).
78. AA Gillespie, 'Adolescents, Sexting and Human Rights' (2013) 13 *Human Rights Law Review* 642.
79. V Dodd, 'Police Chief Convicted of Having Child Sexual Abuse Video on Phone' *The Guardian* (20 November 2019) 25; V Dodd, 'Top Officer in Child abuse Video Case Faces Sack before Appeal' *The Guardian* (11 December 2019) 24; V Dodd, Highly praised officer is sacked by Met over abuse video conviction' *The Guardian* (14 March 2020) 27.
80. Letter dated 31 July 2012 from James Eke, Foreign Policy and Security Group, British Embassy, Washington, D.C., but treated as 'current and verified as of 15 November 2018' in the International Centre for Missing & Exploited Children, *Child Sexual Abuse Material: Model Legislation & Global Review* (ICMEC, Alexandria VA 2018) ii, 58.

This can be compared with how, for example, German law (backed by significant financial penalties and without an industry-financed regulatory intermediary) requires social media platforms to remove 'manifestly unlawful' content within a specified time.[81] With Brexit, but possibly not (see below) with a UK-US trade deal, the UK need no longer be bound by EU law that has privileged competitive claims made on behalf of the ITC industry.[82] Government deference to internet commercial interests and unwillingness apparently to adequately finance legal intervention is clear from the contrast with the often strict corporate liability under English law for many health and safety offences or even, at a higher threshold for legal intervention, obscene theatrical performances.[83]

Limits to Collaboration—ACNs, the Deep Web, ISPs That Are Beyond Regulation and Social Media Platforms 'Going Dark'

This section explains the limits of what is apparently achievable through government-industry accords for image suppression on the surface web by considering how criminals exploit platforms and communication networks that (a) cannot be regulated (ACNs and surface web services operated from countries that are relatively safe for cybercriminals[84]) and (b) are not regulated (but could be) such as commercially provided encryption, for example, Signal ('going dark') and police responses. This includes the combination of anonymization techniques, for example, the combined WhatsApp and ACN connectivity revealed by Operation Tantalio's investigation into IIOC distribution.[85] Consideration of these issues also underlines how policy inconsistency between criminal justice interventions on the surface web (for which the Government appears to have a limited appetite) may weaken the policing of anonymised web communication. This is a domain where successive governments have strengthened the role and surveillance powers of the state and where this Government wishes, as will be considered in the next section, to go much further.

It is obviously even more difficult to estimate the scale of IIOC offending on ACNs than on the surface web or the volume of crime that uses a combination of different web levels, or the volume of IIOC images involved:

> . . . virtually all reports made to the [NCMEC] CyberTipline relate to content that is being shared, stored, and distributed on the open web, not the dark web. . . . though NCMEC is aware that the dark web is increasingly where new, and virulently explicit, child sexual exploitation content is solicited, traded, and discussed among predators.[86]

81. Communications Committee, *Regulating in a digital world* (HL 2017–19, 299) paras 183–185 indicated that it was clear from this example that Art 15 of *Directive 2000/31/EC Directive on electronic commerce* [2000] OJ L 178/0001, which ensures online intermediaries are not liable for illegal content found on their services, is not a barrier legally to such a law enforceable with substantial financial penalties. With Brexit, but possibly not (see below) with a UK-US trade deal, the UK could go much further in bringing the industry within the scope of criminal and civil proceedings for non-compliance with IIOC policing and social regulation requirements.
82. For example, Case C-70/10 *Scarlet Extended SA v SABM* [2011] ECR I-12006 determined that an ISP could not be required to prevent its users from downloading copyright protected works without authorisation and without paying royalties via peer-to-peer networks.
83. 'Where any offence under this Act committed by a body corporate is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of [senior corporate staff], he as well as the body corporate shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly': Theatres Act 1968s 16.
84. For the latter see: J Lusthaus, *Industry of Anonymity* (Harvard UP, Cambridge MA 2018) 181–189.
85. Led by the Spanish police, 18 agencies identified 130 suspects in 15 countries: Europol, *Press Release 18 April 2017* 'Global action tackles distribution of child sexual exploitation images via WhatsApp: 39 arrested so far, <https://www.europol.europa.eu/newsroom/news/global-action-tackles-distribution-of-child-sexual-exploitation-images-whatsapp-39-arrested-so-far> accessed 11 December 2019.
86. Shehan (n 56) 2–3.

The IWF has suggested that less than 1% of child sexual abuse URLs is on ACNs.[87] However, the Home Office estimated in 2019 that 140,000 user accounts registered on the worst child abuse sites on ACNs are located in the UK.[88] Such sites have many users: a single ACN child abuse site hosted in Queensland ('The Love Zone') had 45,000 members.[89]

Image suppression on the regulated parts of the surface web may be less effective in curbing crime than might be hoped. During 2014 Microsoft and Google achieved a 67% reduction in child sexual exploitation searches in the USA, but the Russian based search engine Yandex was known to have been used by American residents. Empirical research into whether, how and to what extent police and commercial interventions against cybercrime result in displacement is at an early stage. The authors of one pioneering study (financial not IIOC crimes) noted, however, the creativity of cyber criminals and concluded that effective police and private sector responses can result in at least some displacement that takes different forms (e.g. from personal bank accounts to corporate targets and from banks in one country where security is strong to those where crime prevention is weak).[90] This problem is not really addressed in *Online Harms*, although the known displacement of terrorist activity to less hostile locations as a result of more intensive effort by companies to supress extremist content is acknowledged.[91] What is particularly troubling about potential cross-border IIOC crime displacement on the surface web is that commercial benefits would accrue to the new platform hosts. More users translates into increased advertising revenue for sites that do not take down such images, as noted in another path-finding study of criminal displacement, on the internet 'further monetizing the sexual exploitation of children'.[92]

The potential relationship between the legal impact of the future *Online Harms* legislation and internet policing in domains beyond regulation, however, might also extend to equipment interference ('hacking') and distributed denial of service attacks (DDOS), both of which are lawful and like bulk data analysis subject to oversight by the Investigatory Powers Commissioner's Office (IPCO).[93] These exceptional state activities also provide important precedents for how criminal law may override the legal privileges that the digital industry enjoys under commercial and regulatory law.

UK policing and harm reduction on other domains, including encrypted communications interception is undertaken by the state agencies, chiefly the National Crime Agency (NCA) and individual police forces supported by regional crime units, the intelligence services and specialist agencies such as HM Revenue and Customs. Their work has an operational link with the surface web collaboration arrangements and will involve the same industry or NGO participants. For example, when ACN sites hosting IIOC material are taken down the NCMEC assists in this process by identifying first-generation seized images that had not been previously been logged in their IIOC database, and already shared nationally and internationally with police agencies and or other specialist child protection NGOs.[94] Criminal justice interventions, however, are not dependent on voluntary assistance. For example, bulk data analysis (the analysis of communication footprints, often on the deep web (e.g. bank account records) but also on the surface web, enables state agencies to identify clusters of criminal activity in order to identify UK

87. IWF (n 7) 32.
88. T Pilgrim, 'Javid announces 'game-changing' tech to boost fight against online child abuse' *Care Appointments* (12 July 2019) <https://careappointments.com/care-news/england/130086/javid-announces-game-changing-tech-to-boost-fight-against-online-child-abuse/> accessed 3 February 2020.
89. SD Brown 'Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice' (2020) 20 *ERA Forum* 428.
90. F Jansen and J van Lenthe, 'Adaption Strategies of Cybercriminals to Interventions from Public and Private Sectors' in TJ Holt (ed), *Cybercrime through an Interdisciplinary Lens* (Routledge, Abingdon 2019) 210–41.
91. DDCMS and Home Office (n 9) para 1.10 and 14 (Box 2).
92. CMS Steel, 'Web-based Child Pornography: The Global Impact of Deterrence Efforts and its Consumption on Mobile Platforms' (2015) 44 *Child Abuse & Neglect* 157.
93. See Brants et al. (n 35) and Davies (n 35) in this issue for the legislation and discussion of ICPO's oversight role.
94. US Justice Department, *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin* (16 October 2019) <https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child> accessed 16 April 2020.

citizens who pay to access extreme IIOC material.[95] This is permitted by statute and because such surveillance engages Convention privacy and sometimes fair trial rights, the law requires that it should be supervised by IPCO, to ensure that such powers are used proportionately.[96]

Judgements about proportionality can pivot on the weight attached to the public objective, expressed in another common law jurisdiction as a 'sufficient importance' test.[97] It may be arguable that an absence of policy consistency—including (judging by current statistical trends) over resource allocation to maintain or increase criminal justice interventions together with irresolution about seeking effective powers to require industry action where less invasive techniques can be used (e.g. on the surface web)—might weaken a proportionality claim to justify the use of exceptional measures against an ACN, surface web encryption, or a platform well beyond UK regulation. It would certainly be difficult to reconcile a claim that the state must always be able to intervene with the full force of the criminal law against IIOC crimes in such domains, when (a) its policies only allow for very limited and diminishing criminal justice interventions on the unencrypted surface web where most IIOC images are to be found and (b) even uncooperative corporate entities enjoy impunity from prosecution or exceptional protection from civil litigation.

Such exceptional activities have a further link with the impact of neoliberal policies on criminal justice: how government technological development and research capabilities on which police and other state agencies at one time relied are now either seriously inadequate or non-existent.[98] As a result the police and other government agencies rely on the marketplace for hacking devices and services. A law suit brought by WhatsApp/Facebook against NSO, an Israeli cybersecurity device developer in October 2019 exposed some of the risks arising from this. It was alleged that NSO's malware product Pegasus[99] had been used against diplomats, senior government officials, human rights activists, dissidents and journalists, including people linked to the Saudi journalist, Jamal Khashoggi, who was assassinated inside the Saudi consulate in Istanbul. Allegedly it is effective against many commonly used smartphone operating systems, including Apple's iOS, Google's Android, Microsoft's Windows Phone and Samsung's Tizen. NSO's response was that it did not itself use malware operationally and that its state security agency customers could have their use of the malware stopped for a breach of licence conditions. That, of course, does not answer the obvious question: would such a breach be reported by such customers?

The litigation revealed how a combination of neoliberal policies—fiscal austerity, the hollowing-out of state capabilities and minimal regulation—has resulted in revenue from state agencies funding the commercialised development of advanced surveillance devices and services that may be acquired by rogue states and criminals. According to *The Wall Street Journal*, the publicity from the Pegasus affair compromised a criminal justice investigation into suspected anti-terrorist activity.[100] Similarly, Home

95. GCHQ, 'GCHQ and NCA Join Forces to Ensure No Hiding Place Online for Criminals' (6 November 2015) <https://www.gchq.gov.uk/news/gchq-and-nca-join-forces-ensure-no-hiding-place-online-criminals> accessed 31 March 2020.
96. Investigatory Powers Act 2016 (IPA) pt 6.
97. The Canadian *Oakes* test requires an objective 'of sufficient importance to warrant overriding a constitutionally protected freedom', K Moller, 'Constructing the Proportionality Test: An Emerging Global Conversation' in L Lazarus, C McCrudden and N Bowles (eds), *Reasoning Rights: Comparative Judicial Engagement* (Oxford, Hart 2016) 34.
98. The situation in England and Wales is now so dire that when the Government appointed Forensic Science Regulator (FSR) arranged an initial validation study of commercially sourced kiosks used by the police to extract and begin to analyse data held on a device, the results could not (initially at least) be fully disseminated to police forces and no mechanism was available to keep that work up-to-date: FSR oral evidence, Science and Technology Committee, *Forensic science and the criminal justice system: a blueprint for change* (HL 2017–19 333) Q209.
99. After dialling the target phone, even if it is not answered, it is claimed that encrypted content can be accessed. Pegasus was said to have been used against 1,400 mobile phones across 20 countries.
100. This story has been reported extensively on the Deutsche Welle (DW) website: 'WhatsApp attacked by advanced spyware via missed calls' (14 May2019) <https://www.dw.com/en/whatsapp-attacked-by-advanced-spyware-via-missed-calls/a-48726819>; D Regev, 'WhatsApp attacked by advanced spyware via missed calls' (17 May 2019) <https://www.dw.com/en/whatsapps-security-breach-made-in-israel-implemented-worldwide/a-48740524>; 'Whatsapp sues Israeli company over spyware scandal' (30 October 2019); L Sanders IV, 'Israeli Spyware Firm Threatens to "Shut Down" Abusers' (9 February 2020), accessed 4 March 2020.

Office evidence to IICSA indicated that one ACN site required its subscribers to upload 20 'first-generation images', as an alternative to a two-minute video of infant or toddler abuse, each month.[101] Unless there was an element of bluff to this, presumably the criminals involved were able to access the same or similar image analysis software as that used internationally by police, intelligence services and anti-abuse NGOs, or as a result of corruption, an image suppression database.

The Future Evolution (and Its Potential Limitations) of the Collaborative Justice Interventions and Harm Reduction Model

The Online Harms White Paper

The premise of UK Government's *Online Harms White Paper* (April 2019)[102] is that the current voluntary collaborative justice and harm reduction model is failing:

> There is currently a range of regulatory and voluntary initiatives aimed at addressing [online harms], but these have not gone far or fast enough, or been consistent enough between different companies, to keep UK users safe online.[103]

The term 'online harms' covers an extensive range of 'illegal or unacceptable content and activity' on the surface web, ranging from the availability of illegal images (including IIOC) to 'unacceptable behaviours' (e.g. social media algorithms that create 'echo chambers' or 'filter bubbles') or some forms of commercial exploitation (e.g. designed addiction to digital services).[104]

These problems are to be addressed by the creation of an overarching state authority that will empower an independent regulator to impose duties on the industry to undertake social regulation over surface web services, including IIOC image suppression, in order to reduce the risk of harm for users. This would undoubtedly be an improvement on the current voluntary and variable collaborative arrangements on which the police rely for assistance with IIOC crimes. The *Online Harms* proposals, however, are concerned primarily with influencing commercial behaviour, including industry-customer relations, and conceived in a policy making environment with expertise in the regulation of commercial entertainment or consumer services. This can be seen in how the Government's proposals for 'user redress' envisage 'an independent review mechanism to ensure that users have confidence that their concerns are being treated fairly'.[105] This is a far cry from action against IIOC offenders and the level of harm suffered by their victims.

IICSA published an investigation report about the nature and extent of the use of the internet to facilitate child sexual abuse in March 2020.[106] This called for a more effective response to IIOC,[107] expressing specific concerns about both the corporate response to live streamed child abuse and the uncertain pace of the Government's implementation of its *Online Harms* plans:

> We are unconvinced that internet companies fully understand the scale of the problem of live streaming on their platforms such that they can properly assess whether they employ sufficient numbers of moderators to detect such offending.[108]

101. IICSA (n 24) 17.
102. DDCMS and the Home Office (n 9). This reference also cites evidence of the intended continuity of the proposed policies under the Johnson Administration.
103. Ibid para 8.
104. Ibid paras 2–6.
105. DDCMS and Home Office (n 9) 3.26–3.30.
106. IICSA (n 24).
107. Ibid 2 and para 95.
108. Ibid 3.

> The Online Harms proposals are wide-ranging but the timetable for implementation of this legislation is unclear. The prospective interim code of practice in respect of child sexual abuse and exploitation offers a very real opportunity to make children in the UK safer online.[109] We therefore unhesitatingly recommend that the interim code is published without further delay.[110]

IICA also noted how 'encryption poses a real risk to the ability of law enforcement to detect and investigate online-facilitated child sexual abuse'.[111]

Critique of the Online Harms White Paper from the Perspective of IIOC Issues

US commercial considerations and neoliberal hostility to regulation could negate this initiative. It was suggested in Parliament during 2019 that the required observance of some aspects of US commercial internet law in the US trade agreements with Canada, Mexico and Japan, if applied to a post-Brexit UK-US trade deal, 'would basically wipe away all the [proposed *Online Harms*] legislation'.[112] Even if the proposals are abandoned or significantly modified, the value of examining them in their original form is that at this early stage the neoliberal assumptions or mind-set reflected in the policy document is likely to be most apparent. This is done by considering whether *Online Harms* is really likely to result in a fundamental break with earlier neoliberal reluctance to interfere with the free market relating to the internet by considering four issues, evidence of intent, funding, regulatory compromises over innovation and smaller enterprises, and regulator designation.

For anyone hoping for evidence of a decisive shift in Government thinking about how to deal more effectively with IIOC crimes, a general concern arises from its significantly more circumspect (or reluctant) criticism of voluntary arrangements than near contemporary NCMEC evidence to the US Senate:

> . . . many technology companies that embrace their societal and corporate responsibilities to manage content on their platforms and to actively detect and remove child sexual exploitation content . . . [However,] too many companies are not proactive in fighting this insidious problem of online child sexual abuse material and engage in half-measures, decline to participate in voluntary initiatives or information-sharing opportunities, and too often put child protection secondary to organizational financial and broader liability concerns.[113]

There is certainly no sign of a diminution in neoliberal influence over funding plans. Consistent with even UK physical border security (another Home Office responsibility),[114] the new collaborative model system is likely to continue to rely on user-generated revenues and little or no support from taxpayers.[115] For online protection as much as border control, the Government's eventual fiscal objective is described, in classic neoliberal language, as a 'cost neutral' solution (no net public sector funding).[116]

109. Ibid 3.10: The codes to which it refers in its report concern both child abuse and anti-terrorism measures. The Government envisages taking powers to issue direct to the regulator about their content and to approve draft codes before they are brought into effect. It is envisaged that the regulator will not normally permit companies exemptions from observing these and would 'require a high burden of proof that alternative proposals will be effective'.
110. Ibid 3.
111. Ibid 2.
112. Digital, Culture, Media and Sport Committee, *Oral evidence on 16 October 2019: The work of the Department for Digital, Culture, Media and Sport*, HC 2019 71) Q627.
113. Shehan (n 56) 3.
114. Wilson (n 59) 5–6.
115. 'The regulator will be funded by industry in the medium term, and the government is exploring options such as fees, charges or a levy to put it on a sustainable footing. This could fund the full range of the regulator's activity, including producing codes of practice, enforcing the duty of care, preparing transparency reports, and any education and awareness activities undertaken by the regulator'. DDCMS and the Home Office (n 9) para 37.
116. Ibid 98; Wilson (n 59) 6.

Significant compromises in the *Online Harms* regulatory regime also reflect neoliberal assumptions. For instance, the Government would not participate directly in economically sensitive decisions while instructing the independent regulator about how it should balance public goods against commercial arguments when exercising its new powers:

> We would expect the regulator to . . . [support and encourage] innovation . . . , subject to minimum expectations of user safety. . . . to take a flexible, proportionate and risk-based approach when setting and enforcing expectations and responsibilities for companies.[117]

The issues can be complex, with limited empirical research to guide the regulator. It appears, however, that for both data protection[118] and social regulation generally,[119] regulation can boost as well as hinder competiveness.

Another significant compromise is differential regulation determined by firm size and a claimed lack of capacity and capability rather than risk of harm:

> Regulation can impose a disproportionate burden on smaller companies. Badly designed regulation can stifle innovation by giving an advantage to large companies that can handle compliance more easily. We are determined that this regulatory framework should provide strong protection for our citizens while avoiding placing an impossible burden on smaller companies.[120]

This reveals an internal contradiction within the *Online Harms* document itself. It draws attention to the known displacement of terrorist activity to less hostile locations ('more permissive and smaller platforms') as a direct result of more intensive efforts by larger companies to supress extremist content. [121] The Government suggests that the solution to such problems is (a) for the regulator to be required to balance the resources of smaller companies against 'the risk and prevalence of harms on their service'[122] and (b) greater support (from larger firms as much as or more than from government) for example, by developing new 'AI products') for free use by smaller companies.[123] Ultimately, this proposed regulatory compromise could still allow some companies to continue to enjoy total legal immunity should they fail to take action against IIOC crimes and, as indicated in the fourth section, indiscriminate access to specialist software and devices carries a significant risk of such resources falling into the wrong hands.

The neoliberal influence over the Online Harms approach can also be seen in the announcement in February 2020 that Ofcom would add *On-line Harms* regulation to its existing television, radio and telecoms remit.[124] This was influenced by Ofcom analysis of how the same content can be subject to different regulatory standards depending on the platform on which it appears. The Government's decision could be anticipated from its emphasis on finding a solution to 'significant gaps in consumer protection' for the commercially provided services considered in *On-line Harms*.[125]

Irrespective of the general merits of this choice of Ofcom, this body may not be a suitable regulator for dealing with criminal justice issues. Technical reservations about the Government's decision can be found in industry views about regulatory structures for the internet:

---

117. Ibid para 5.11.
118. N Martin, C Matt, C Niebel and K Blind, 'How Data Protection Regulation Affects Startup Innovation' (2019) 21 *Inform Syst Front* 1307–1324.
119. Department for Business, Energy & Industrial Strategy (BEIS) *Research Paper Series Number 2020/002: Innovative Businesses' Views on the Regulatory Environment and Regulatory Support* (BEIS, London 2020).
120. DDCMS and Home Office (n 9) 56 (Box 26).
121. Ibid para 1.10 and 14 (Box 2).
122. Ibid para 7.12.
123. Ibid paras at para 8.9 and (Box 28) (page 79), for how this was done by the industry provided anti-grooming tool.
124. HL Deb 12 February 2020, vol 671 cols 27-28WS.
125. DDCMS and Home Office (n 9) 2.8.

a. Simply adapting, modifying or extending the core capabilities of a traditional regulator is insufficient when introducing internet regulation, as highly specialist proficiency in data, operations, and online content' will also be required.[126]
b. Regulation might be more effective if based on specific 'sectors' which all have a separately designated regulator with sector specific expertise.[127]

Interestingly, these views are in fact consistent with the regulatory and supervisory structure that has emerged within criminal justice. Because separate regulators (e.g. the Forensic Science Regulator (FSR), the Bioinformation Commissioner and the Information Commissioner) and inspectorates (e.g. HMICFRS and the CPS Inspectorate)—each with different specialist foci and skills involving the police or police related matters—liaise closely and regularly engage in joint projects, multiple and overlapping regulation does not result in a dysfunctional system.[128]

Given the importance of the private sector harm reduction and criminal justice intervention interface, concurrent or possibly more extensive powers to those to be conferred on Ofcom are likely to be required for criminal justice bodies that might need to engage in direct inspection and supervision of industry and NGO practice and policies. Probative and procedural problems will inevitably arise at the interface about the reliability, accuracy, comprehensiveness and interpretation of data received from industry and NGOs. These may need to be resolved through inspections, thematic studies guidance from variously or jointly HMICFRS, the CPS inspectorate and the FSR. Likewise, while there is disagreement among legal scholars about when surveillance of public messages on social media engages the right to privacy, it is likely that a systematic analysis of all messages to identify the sharing of IIOC images would do so.[129] Such activities cannot be entrusted to private companies or NGOs without direct public supervision and inspection. An obvious solution would be to give IPCO a supervisory and inspectorate role. The *Online Harms* arrangements will inevitably engage Convention privacy and sometimes fair-trial rights. ICPO has the judicial authority and inspectorial experience to enforce-compliance with Convention rights in police and other regulatory interventions at all levels of and locations on the web.

A Government-Industry Encryption Key Accord?

Zuboff's account of how government-industry accords can extend surveillance without regard to privacy safeguards,[130] demonstrates the major risks arising from various initiatives to negotiate encryption key ('backdoor access') to encrypted communication. A 2019 initiative to achieve this was organised by the Government that directly linked it to IIOC crimes.

The communiqué issued for this initiative by the Five Eyes countries (essentially 'Anglosphere' countries and for that event rebadged as 'Five Countries')[131] veered perilously close to echoing the Sino-Russian surveillance playbook[132] in the link with IIOC crimes:

126. M Bickert, *Charting a Way Forward: Online Content Regulation* (Facebook, Menlo Park CA 2020) 19.
127. Communications Committee (n 81) para 30.
128. A relevant analogy that puts this question in perspective is how expert scientific decisions in the criminal justice system are better served by a complex system of interlocking forms of regulation and how the risk of dysfunctionality is greater when the alternative is the application of ideological purity rather than scientific rigour, see Ward (n 11).
129. Gillespie (n 26) 354.
130. Zuboff (n 54) 112–21.
131. Australia, Canada, New Zealand, USA and UK; the 'Five Country Ministerial: Emerging Threats' meetings involved ministers for home affairs, interior, security and immigration and attorney generals.
132. For an account of 2016 Moscow Sino-Russian event described as 'the industry's prime conference on online child and adult safety' that preceded the extension of Chinese style web censorship and surveillance to Russia, see J Griffiths, *The Great Firewall of China* (Zed Books, London 2019) 247–52.

> 1. In five years, we have seen a near twenty-fold increase in industry referrals of child abuse material . . . , from 1 million in 2014 to over 18 million in 2018. Driven by the moral obligation to tackle this escalating crisis we met representatives from Facebook, Google, Microsoft, Roblox, Snap and Twitter. . . .
>
> 6. . . . it is imperative that all sectors of the digital industry including Internet Service Providers, device manufacturers and others continue to consider the impacts to the safety of children, including those who are at risk of exploitation, when developing their systems and services. In particular, *encryption must not be allowed to conceal or facilitate the exploitation of children* (author's emphasis).[133]

This proposal to bypass encryption, like earlier attempts was rejected by industry. The minsters simply reaffirmed Five Countries—industry voluntary cooperation against online child abuse as 'a set of principles that would help to shine a light on this issue and provide some critical guidance to industry in what they can do to help'.[134] Though what eventually appeared on the Home Office website eight months later was much bolder in tone, referring to the need for 'an immediate upscaling of the global response . . . to ensure that there is no safe space online for offenders to operate'.[135]

The Government's credibility—as the meeting's host and thereby organiser[136]—was in any case swiftly compromised by a decision to transfer Conservative MP communications from encryption protected WhatsApp to the Signal platform.[137] In addition to encryption, Signal's standard commercial offering includes an option for the automatic deletion of all traces of communication even among recipients (the Disappearing Messaging feature) and a 'burner' (dummy account) number can be obtained by signing up to Signal through Google Voice Communication.[138] Ironically, well before Conservative MPs changed their social media brand, the FBI was known to have hacked encrypted Signal messages sent by Congressional officials and journalists.[139]

The industry's arguments against backdoor access are that it would be 'a "gift" to criminals, hackers and repressive regimes'.[140] Certainly the technologically based argument that encryption keys would represent a 'U-turn from the best practices now being deployed to make the Internet more secure' enjoys considerable international support. An increasing international consensus on this is evident from a 2015 report by the Special Rapporteur for the UN Human Rights Council and in the UN General Assembly in

133. Five Country Ministerial: Emerging Threats, London 2019, *Communiqué*, <https://www.gov.uk/government/publications/five-country-ministerial-communique/five-country-ministerial-ommunique-emerging-threats-london-2019> accessed 11 December 2019.
134. New Zealand Department of Internal Affairs (NZDIA) web page, *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse* <https://www.dia.govt.nz/Voluntary-Principles-to-Counter-Online-Child-Sexual-Exploitation-and-Abuse> accessed 17 April 2020.
135. Home Office, *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse* (5 March 2020) <https://www.gov.uk/government/publications/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse> accessed 17 April 2020.
136. Based on the author's contribution when a senior civil servant to UK hosted EU presidency and G7 meetings.
137. The party argued that following the 2019 Election that the number of Conservative MPs exceeded the WhatsApp maximum group size. J Waterson, 'MPs Switched from WhatsApp to Stop Leaks' *The Guardian* (18 December 2019) 11.
138. J Knight, *Four Ways to Hide All Traces of your Message Using Signal Private Messenger*, 2 June 2018 <https://smartphones.gadgethacks.com/how-to/4-ways-hide-all-traces-your-messages-using-signal-private-messenger-0182633/> accessed 19 December 2019.
139. L Hay Newman, 'Encrypted Messaging Isn't Magic', *Wired*, 14 June 2018 <https://www.wired.com/story/encrypted-messaging-isnt-magic/> accessed 19 December 2019.
140. C Hymas, 'Facebook rejects Priti Patel's calls to open up encryption to help in fight against terrorists and child abusers' *Daily Telegraph* (10 December 2019) <https://www.telegraph.co.uk/politics/2019/12/10/facebook-rejects-priti-patel-calls-open-encryption-help-fight/> accessed 14 January 2020. This is the same argument used by Apple in rejecting a FBI request to assist that agency to bypass encryption in 2016, Apple, *A Message to Our Customers* (16 February 2016) <https://www.apple.com/customer-letter/> accessed 4 May 2020.

2016, which is supported by the International Association of Chiefs of Police (IACP).[141] In addition there are strong grounds for public distrust, manifested for example in greater use of ACNs and the clear trend of the internet darkening. This will reflect in part the impact of the Snowden revelations.[142] Regaining public trust to resolve the encryption key issue will also be more difficult because of a better public understanding (thanks to scholars such as Zuboff) of the trade-off to abandon industry regulation in return for hidden surveillance assistance.

There may, however, now be common ground that allows a way forward on the encryption key issue for both governments and industry. For the industry, the NSO litigation was effectively a game changer as Facebook, in an unprecedented move, had fully acknowledged the vulnerability of commercial encryption services. As far as governments are concerned the risks of police and intelligence agencies procuring technological development, devices and services in an unregulated market place are equally exposed now that it can be seen as an enabler of serious crime. Both sets of interests have been damaged by the wider consequences of neoliberalism and would benefit from legislative arrangements that provide the degree of judicial and democratic supervision and transparency required to establish critical trust among informed citizens.

Conclusions

The encryption key impasse might be resolvable by building on the powers introduced in 2000 for the judicial authorisation of access to protected information on, for example, a suspect's telephone (protected by an encryption key or password) under arrangements overseen by IPCO.[143] Facebook - although it does not use the terms - appears to have given considerable attention to the need to improve critical trust and to have grasped the lessons of civic epistemology. Even if its apparent change of heart towards the acceptance of *Online Harms* type social regulation, is a result of 'tech lash', from customers/users frustrated over how web platforms profit from their data at a time when in its most important markets, USA and Canada, user growth is stagnating,[144] in other words evidence of the potential influence of 'an issue-specific public'.[145] Certainly its publication about future internet services regulation is much more sensitive to the wider question of restoring public trust than the Government's *Online Harms* document. Facebook acknowledges the importance of legal structures and procedures for building trust among citizens who might have good reason to have lost faith in both government and the digital industry:

> Problems arise when people do not understand the decisions that are being made or feel powerless when those decisions impact their own speech, behavior, or experience. People may expect similar due process channels to those that they enjoy elsewhere in modern society.[146]

It acknowledges public nervousness of regulatory arrangements that lack the transparency of the legislative process in democratic countries, 'with due respect for human rights and, critically important for reducing the likelihood of capricious restrictions on legitimate speech, the check of an impartial

141. M Gutheil, Q Liger, A Heetman, J Eager and M Crawford, *Report for the Directorate General for Internal Policies Policy Department C: Citizens' Rights And Constitutional Affairs Civil Liberties, Justice And Home Affairs Legal Frameworks for Hacking by Law Enforcement* (European Parliament, Brussels 2017) 21–24.

142. EA Jones and E Martellozzo, 'Introduction: Victims of Cybercrime in the Small "I" Internet' in E Martellozzo and EA Jones (eds), *Cybercrime and its Victims* (Routledge, Abingdon 2019) 9.

143. The Regulation of Investigatory Powers Act 2000 (RIPA), Part 3; see also, *R v S and another* [2008] EWCA Crim 2177, [2008] All ER (D) 89: (a) self- incrimination protection is not an absolute right and (b) does not apply to evidence which has an existence independent of the person who holds the key.

144. N Drozdiak and Bloomberg, 'Facebook CEO Zuckerberg looks to calm 'tech lash' with call for government rules on political ads and data' *Fortune* (17 February 2020) <https://fortune.com/2020/02/17/facebook-ceo-zuckerberg-eu-government-regulation/> accessed 17 February 2020.

145. Jasanoff (n18).

146. Bickert (n 126) 3–4.

judiciary'.[147] There are grounds for caution about Facebook's current position not least now that it is understood how free speech and privacy concerns were exploited at the end of the previous century to evade regulation.[148] Effective deliberative engagement with citizens and their representatives over a balanced approach to these human rights issues will be critical in obtaining support for finding a democratically acceptable way forward.

On specific issues relating to IIOC crimes, the analysis in this article also points to the importance of bringing into any future deliberations about surface web regulation and encryption other issues: preventing the hollowing out of criminal justice capacity and capabilities; ensuring compatibility and consistency in operational responses and legal principles when dealing with IIOC crimes across all levels of the web; and ensuring that the response to IIOC crimes focuses on the offenders and their victims by accepting that image suppression alone is insufficient.

This article has attempted to offer an informed and constructive critique of the evolution and potential future of collaborative justice and harm reduction in response to IIOC crimes as' something to be explained, not to be taken for granted'. It has sought to highlight potential 'strategic deletions and omissions'. In doing so it has emphasised the significance of genuine political and policy choices that will determine how IIOC crimes are dealt with. In doing so it has warned against any mind-set that considers or argues that decisions on and developments in technologically and scientifically focused decision making are so determined by apparently impersonal economic and technological forces, that there is no alternative to whatever government can negotiate with vested interests behind closed doors.

Acknowledgements

Comments on earlier versions of this paper from Dutch, Norwegian, Swedish and British research project colleagues, especially Professor Chrisje Brants, and Mark Ashley Parry's research assistant support at a NPCC sponsored conference held in November 2019 are gratefully acknowledged.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The author(s) received financial support for the research, authorship, and publication of this article from NordForsk, the Economic and Social Sciences Research Council (ESRC) and the Netherlands Organisation for Scientific Research (NWO) as funding for Police Detectives on the TOR-network: A Study on Tensions Between Privacy and Crime-Fighting (project no. 80512).

147. Ibid 16.

148. See the extensive literature about s 230 of the Communications Decency Act (CDA) 1996 and *Reno v. ACLU* 521 US 844 [1997]. The author is more sympathetic than Zuboff (n 54) 107–112, however, to the arguments made on behalf of some of the litigators in *Reno* and the outcome of that case.