Secrecy and surveillance: lessons from the law of IMSI catchers

Paul F Scott*

1. Introduction

The modern technological era creates a variety of new possibilities for law enforcement bodies, which they have not been slow to exploit. The law, however, has not always kept pace with these developments, so that – for instance – equipment interference by the police and the security and intelligence agencies for a long time took place on the basis of general powers of 'property interference' whose use to that end was not obviously foreseeable.[1] Only following the Snowden revelations of 2013 did the enactment of the Investigatory Powers Act provide a more solid, more transparent legal basis for such actions, along with others which were already taking place on the basis of dubious legal authority.[2] One problem of accountability in the context of modern surveillance techniques has therefore been an uncertainty as to the law: what is permitted by vague, or obscure, or repurposed, legal provisions. The other side of the accountability coin is an uncertainty as to fact: that is, it is difficult verging on impossible to ensure effective accountability even where the law is suitably clear, and suitably accessible, if we do not have sufficient knowledge of the relevant factual matrix to which it is or might be applied. Accountability is weakened, perhaps wholly undermined, by this epistemological shortfall.

This piece explores this theme in the context of a consideration of the law as it applies to the use of 'IMSI catchers' (often known – in the United States in particular – as 'Stingrays')[3] as used both in prisons – in relation to which there exists a series of additional or distinctive powers – and generally. It shows that the legal basis is a mixture of the weak and the contestable, susceptible to challenge on both 'domestic' and ECHR grounds. Moreover, the multiple uses to which IMSI catchers might be put demonstrate the limitations for accountability of a legal

[1] See the discussion in Paul F Scott, 'General Warrants, Thematic Warrants, Bulk Warrants: Property Interference for National Security Purposes' (2017) 68 *NILQ* 99.

[2] Scott (n 1) and Paul F Scott, *The National Security Constitution*, Hart Publishing (2018), ch 2.

[3] StringRays are manufactured by the Harris Corporation of Melbourne, Florida, and were introduced in 2001 and later succeeded later by the StingRay II. A number of other devices are also manufactured by the same firm. One of these, the Triggerfish, predates the StingRay, and was famously used to locate wanted hacker Kevin Mitnick in 1995: see Nicole Valdes Hardina, 'Uncovering the Secrecy of Stingrays: What Every Practitioner Needs to Know' (2018) *Criminal Justice* 20. A more advanced version of the StingRay, known as HailStorm, now also exists and appears to be oriented towards the Long-Term Evolution (LTE) standard for wireless communication which has been progressively introduced in the last decade and which complicates the use of IMSI catchers due to its superior security protocols. In discussing 'IMSI catchers' I refer to the entire range of devices with equivalent functionality.

approach, like that which prevails in the United Kingdom, which divides up investigatory powers by their effect. A multi-use device such as an IMSI catcher, capable of slipping from one regime to another with little more than a twist of a dial, is, in this landscape, liable to fall through the cracks: being potentially subject to all regimes of investigatory powers, it is in reality as likely to be subject to none of them at all. For both these reasons, amongst others, IMSI catchers operate as a case study in the weaknesses of the contemporary legal regulation of surveillance technology even after the rationalising project undertaken by the 2016 Act. Most importantly, however, it is only the pervasive secrecy surrounding both the fact of IMSI catchers' use, and the ways in which they are and might be used, which has allowed such use to go – so far – unchallenged. IMSI catchers are a case study in the weaknesses of the modern UK approach to surveillance powers, whereby the law is now (mostly) clear and rational, but the facts to which that law applies are kept as far as possible behind a veil of secrecy which weighs against that legal improvement. The existence of IMSI catchers is of course well known: what is important about them as a case study is that all of the failings of accountability (legal and political) that apply in relation thereto must by definition exist – and indeed be more complete – also in relation to other technologies, the existence of which is as yet unknown.

2. Background: the emergence of legal clarity

This section very briefly outlines the trajectory of the development of law in the area of secret surveillance,[4] showing that the trend has been towards more law, more accessible law, and clearer law. The first statutory interception provision appears to have been section 4 of the Official Secrets Act 1920, the import of which was not generally appreciated until publicised by journalist Chapman Pincher in the late 1960s.[5] Only following the decision of the Strasbourg Court in *Malone v United Kingdom* was provision made for the interception of internal communications,[6] by the Interception of Communication Act 1985. The powers thereunder were replaced by a broader set of powers under the Regulation of Investigatory Powers Act 2000, a statute whose complexity was legendary,[7] and the meaning of key provisions of which was not fully appreciated

[4] On which, see more fully Scott (n 2) chapter 2. See also C Moran, *Classified: Secrecy and the State in Modern Britain* (Cambridge, Cambridge University Press, 2012), chapter 4.
[5] The story of the revelation and the government's counterproductive response is told in P Hedley and C Aynsley, *The D-Notice Affair* (London, Michael Joseph, 1967).
[6] *Malone v United Kingdom* (1984) 7 EHRR 14.
[7] 'Unfortunately, however, RIPA itself is complex, fragmented and opaque. It is extraordinarily difficult both to understand and to apply' David Anderson QC, *A Question of Trust*: *Report of The Investigatory Powers Review* (2015), [12.20].

for more than a decade afterward.[8] Clarity came only in the course of litigation prompted by the Snowden revelations[9] – litigation which also resulted in the disclosure for the first time of internal arrangements relating to the use made of intercepted material and which is key to the question of whether surveillance measures are compatible with the Convention on Human Rights.[10]

What also became apparent in this period, however, was that a number of obscure or vague provisions of certain statutes were being used to ground surveillances practices which were not, and in some cases could not have been, predicted even by knowledgeable observers of the relevant legal regimes. Three such practices are key. The first is the use by the security and intelligence agencies of 'bulk personal datasets' – databases, acquired via any one of a number of avenues, which contain personal data relating to persons the majority of whom are not, and never will be, of interest to the security services. The use of such 'BPDs' took place under the dubious authority of what are known as the 'information gateway provisions' of the Security Service Act 1989 and Intelligence Services Act 1994, notwithstanding that the terms of those provisions given no indication of any such practice.[11] The second, again based on the 1994 Act (alongside the Police Act 1997) is the practice of 'equipment interference' – most importantly, computer hacking – which was carried out on the basis of powers to interfere with property,[12] and which was held by the Investigatory Powers Tribunal to be a foreseeable use of those powers by reference to comments made during debate on what became the Computer Misuse Act 1991.[13] The third practice was the acquisition (in bulk) of communications data (roughly

[8] See, most importantly, the witness statement of Charles Farr, then Director of the Office for Security and Counter-Terrorism, in case IPT/13/92/CH (16 May 2014), in which the meaning of 'communication' as understood by the state, as well as the significance of the distinction between 'internal' and 'external' communications, was outlined publicly for the first time.

[9] See Jemima Stratford and Tim Johnston, 'The Snowden "revelations": is GCHQ breaking the law?' [2014] *EHRLR* 129.

[10] See *Weber and Saravia v Germany* (2008) 46 EHRR SE5, in which they were most famously articulated.

[11] See Scott (n 2) 97-103.

[12] See Scott (n 1).

[13] *Privacy International v The Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIP Trib 14/85-CH, [81]. The key part of the debate is as follows: 'As the House knows, the Security Services Act legalised burglary through a warrant signed by the Secretary of State. That was highly contentious legislation, opposed by many and severely criticised by all parties, including some Conservative Members. The hon. Members for Thanet, South (Mr. Aitken) and for Aldridge-Brownhills (Mr. Shepherd) made strong cases against it. I am sure that most hon. Members thought that the warrant allowed the security services physically to break into premises, as long as they did not commit another offence. I emphasise the word "physically" because, as I understand it, under the terms of the warrant, the authorised person can invade premises in that way. Until the Minister spoke in Committee there was no sign that the warrant could authorise MI5 staff to hack into any computer whenever they wanted, without committing this Bill's proposed offence of unauthorised access. That power to give a warrant to legalise computer hacking was not discussed in debates on the Security Services Act. The way in which the matter is being

what is in other contexts called metadata) on the basis of the authority of section 94 of the Telecommunications Act 1984, the existence of which had been noted in passing (and the use of which had been speculated) but whose centrality to the post-September 11 regime of surveillance was unknown and unknowable until it was avowed by the executive as part of the reform of the law of investigatory powers.[14] All three of these powers will be overtaken by the Investigatory Powers Act 2016 when it is brought fully into effect.[15]

Though it is not quite a fully comprehensive code for surveillance, the 2016 Act is – unlike that which it supersedes – mostly explicit about the powers it creates and what they permit, as well as the safeguards which apply to those powers and information acquired through their use. Such powers are organised within the act according to their effect, and so the regime is on a formal level neutral as to the technology by which the relevant effect is achieved. Considered together with the various Codes of Practice whose publication the 2016 Act requires,[16] therefore, it seems fair to suggest that the law of surveillance has now addressed what was until recently the most significant of the formal problems associated with it – opinions, of course, will differ as to the substance of the laws. What I argue here, with reference to IMSI catchers, is that this relative clarity and certainty as regards the law is a necessary but not sufficient condition of a tolerable legal regime governing surveillance. To it, we must add something we often do no possess: an adequate grasp of the relevant facts – the techniques and technologies which exist, and are or might be employed – and their relation to the law. In what follows, I make this point with reference to what are known as IMSI catchers, considering first their nature and possible uses, and then some of the questions of law and accountability which arise in relation to such use.

3. IMSI catchers and their use in the UK

3.1. What are IMSI catchers?

pushed through means that the House is being deceived because we are not having a proper debate, and those powers are not being properly restrained and decided on.' HC Deb 4 May 1990, vol 171 col 1300 (Harry Cohen). The specific words quoted by the IPT are found in column 1307, in a contribution by Hugo Summerson, who said also that '[t]here is concern on both sides of the House about the control of the security services. Last year the House passed the Security Services Act 1989. Rightly, the Security Service reports to the Home Office and to the Prime Minister. However, we may need more safeguards to stop the misuse of computers, and it is right that the hon. Member for Leyton should have taken the opportunity to try to introduce additional safeguards.'

[14] See Scott (n 2) 85-97.

[15] Investigatory Powers Act 2016, part 5 and part 6 chapter 3 (equipment interference), part 6 chapter 2 (acquisition of bulk communications data) and part 7 (bulk personal datasets).

[16] IPA 2016, s 241 and schedule 7.

In order to understand subsequent questions of practice and of law, we must understand the basics of the system of mobile telecommunications at issue here. An 'International Mobile Subscriber Identity' ('IMSI') is a number, usually 15 digits in length, which is used to identify the user of a mobile network, to whom it might be matched by a telecommunications provider. An IMSI is usually made up of a 3 digit 'mobile country code', followed by a 2 digit 'mobile network code' and then, making up the remainder of the 15 digits, the 'mobile subscription identification number', which identifies a specific user of the operator in question.[17] It exists alongside two other pieces of information used in mobile telecommunications – encompassing not only the use of mobile phones, but also devices, such as tablets, which communicate in the same way (whether alongside, or instead of, communication over the internet). The first is the International Mobile Equipment Identity ('IMEI')[18] which identifies the device rather than the user – when a person buys a new phone, they will usually associate their subscriber identity with the new device, so that the IMSI stays the same as the IMEI changes. The other is the Temporary Mobile Subscriber Identity ('TMSI'), used in order to provide a degree of anonymity to the user of mobile phones and to prevent their communications from being eavesdropped.[19] Mobile communication networks are made up of a number of geographic zones, in each of which there is some number of 'base transceiver stations', or 'base stations' which connect up to the central communications network.[20] In order to function, a mobile phone must send its IMSI to the network, but the system is designed in such a way that it does so as infrequently as possible.

The devices we are concerned with here operate against this technological background. They are known most formally as 'virtual base transceiver stations' but are more frequently described – in the United Kingdom at least – as 'IMSI catchers'. Litigation relating to the patent for IMSI catchers offers insight into their operation, highlighting two features in particular. The first is that their use 'involves the creation of a false base station' which 'leads the phone to believe that it is genuine, and thereby to communicate with it.'[21] The second such feature 'is the way in which the fake base station causes a mobile phone speedily to transmit to it':

[17] See Jörg Eberspächer, Hans-Joerg Vögel, Christian Bettstetter, and Christian Hartmann, GSM - Architecture, Protocols and Services, 3 ed, Wiley-Blackwell (2009), [3.3.2].
[18] Eberspächer et al (n 17) [3.3.1].
[19] Eberspächer et al (n 17) [3.3.6].
[20] See the overview provided in Eberspächer et al (n 17) [3.1] and [3.2].
[21] *MMI Research Ltd v Cellxion Ltd* [2012] EWCA Civ 7, [5].

> In the normal way phones only link to a base station periodically. The IMSI catcher of the patent works so successfully because it is able quickly to capture the IMSI of the mobile phone. A mobile phone will send a signal when it moves from what is termed one location area code ("LAC") to another… The trick here is to cause the phone to believe that it has moved into a new LAC and therefore communicate with the false base station and deliver up its IMSI. This is achieved by giving the fake base station a different LAC to that of the area where the mobile phone is located.[22]

It is usual to distinguish between the 'passive' and 'active' use of IMSI catchers. In the former case, the IMSI catcher 'simply listens to nearby signals and takes advantage of the initial and unencrypted signals from nearby phones trying to establish contact with a legitimate mobile base station to register which IMSI-numbers are being broadcasted.'[23] On the other hand, an active IMSI catcher 'sends out signals to nearby phones, purporting to be a legitimate base station belonging to their service provider', allowing them to 'gather information from phones even when they are not actively used and can, depending on the configuration "entice" the phone to route communication through the IMSI catcher allowing further collection of communication metadata'.[24] This is often described as a 'man in the middle' attack, and allows access, subject to questions of encryption, to much more than the IMSI of the phone: much of the metadata – data about the communications being made, such as their timing or recipient – but also to the content of those communications.[25]

---

[22] [2012] EWCA Civ 7, [6]. The patent in question, European Patent (UK) No. 1 051 053, has the following abstract: 'A virtual base station (VBTS) with a test mobile telephone (Test-MS) connected to it operates in close range to a mobile telephone (MS). This test telephone detects a list of all base stations near the location by enquiring through the network base station (BTS(Netz)) with the highest power assigned to the selected location. A base station is then selected that is close to t base station with the highest power assigned to the selected location.'

[23] Markus Naarttijärvi, 'Swedish police implementation of IMSI catchers in a European law perspective' (2016) 32 *Computer Law & Security Review* 852, 853. The law in other EU states is addressed in its barest detail in Wanda Mastor, 'The French Intelligence Act: The French Surveillance State' (2017) 23 *European Public Law* 707 and Juan Jose Gonzalez Lopez and Julio Perez Gil, 'The New Technology-Related Investigation Measures in Spanish Criminal Proceedings: An Analysis in the Light of the Right to Data Protection' (2016) 2 *European Data Protection Law Review* 242.

[24] Naarttijärvi (n 23) 854.

[25] The content/metadata distinction has long stood at the centre of the law of surveillance, with all of the relevant law giving effect to the assumption that the content of a communication is more intrusive than is its metadata: to make the point in relation to a telephone call, knowing what was said is more of an invasion of privacy (or whatever other interest) than is knowing what number was called, at what time, and for how long the call lasted. Though nothing here turns on it, much of the contemporary literature contests this assumption and, indeed, it is easy to see how the presence in one's pocket in a device capable of registering one's location (location data being a form of metadata) represents a threat to privacy which is – considered in the round – greater than that associated with access to the content of

The encryption caveat is an important one: the technological basis of mobile communications has evolved rapidly since its entry into the mainstream. The dominant 2G standard for mobile communications (the 'Global System for Mobile Communications' or 'GSM') employed encryption standards now known to be seriously flawed.[26] There was, moreover, a significant gap in its security protocols: though a phone using a 2G signal must authenticate itself to the network over which it wishes to communicate, the opposite is not the case. It is the absence of such a requirement which permits the man-in-the-middle attacks described above. As 2G has been joined – though not yet supplanted – by 3G and 4G networks, these flaws have been addressed in a number of ways. That does not mean that IMSI catchers cease to be of value. For one, the 2G network exists as a fall-back to more advanced networks and one technique employed by IMSI catchers is to block access to those more advanced networks, forcing phones to fall back upon the more vulnerable 2G network.[27] Secondly, it is often the case that even where the content of communications are encrypted the associated metadata is not. More generally, it is clear that those who produce IMSI catchers continue to develop the technology. It is, however, very difficult to acquire details of the technical capacities of newer variants and successor devices, with their manufacturers often – perhaps invariably – insisting that non-disclosure agreements be signed by purchasers of the devices,[28] and the circulation of promotional material being tightly controlled.[29] What is clear, however, is that it would be foolish to assume – in the absence of clear evidence – that technical advances have rendered, or indeed ever will render, the questions under discussion here moot.

3.2. The uses of IMSI catchers

---

particular communications: see, eg, SB Wicker, *Cellular Convergence and the Death of Privacy* (Oxford, Oxford University Press, 2013).

[26] See, eg, Kevin J O'Brien, 'Secret Code Protecting Most Cellular Calls Is Deciphered and Published' *New York Times* (29 December 2009): 'A German computer engineer said Monday that he had deciphered and published the secret code used to encrypt most of the world's digital mobile phone calls, saying it was his attempt to expose weaknesses in the security of global wireless systems.'

[27] Though the 2G networks of a number of states have been shut down in recent years.

[28] For discussion of the legal framework of (non-)disclosure in the United States, see Stephanie K. Pell and Christopher Soghoian, 'Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy', (2014) 28 *Harvard Journal of Law and Technology* 1, 34-40.

[29] A brochure obtained and made public by Privacy International is marked 'cellXion Propietary confidential. Not for redistribution or copying without express permission of cellXion or its approved distributors': cellXion Ltd, product list (nd), hosted at:
https://www.documentcloud.org/documents/810703-202-cellxion-product-list-ugx-optima-platform.html

In advance of considering, as we will do below, the legal regime governing the use of IMSI catchers, it is useful to be as precise (as is possible in the circumstances) about the different ways in which they might be used. The two questions are inextricably linked: the firmness of the legal basis varies significantly depending upon how (and where) the devices in question are used and much of the uncertainty about the legal position which remains is a function of uncertainty on these basic points of fact. We can take them in order of perceived intrusiveness.[30] The first use is simply to identify the mobile phones which are present in a given place at a given time: a key example of such use which emerges from a consideration of the better-developed American literature is where the location of a particular individual is known, but not the details of the mobile phone (or related device) which that person is using, and so it is not possible – without the further information an IMSI catcher can provide – to carry out more traditional interception of communications carried out by that person. This is often linked with the use of what are described as 'burner' phones: those which not registered to a particular user, and which are discarded frequently in order to evade surveillance. It should be noted, however, that an IMSI catcher is not the only way to achieve this end, and others will be preferred where the direction of inquiry is the opposite. So, for example the entirety of the metadata collected by the operators of genuine mobile base-stations during a particular period can also be acquired, something known colloquially as a 'tower dump'.[31] Though a single such dump might be relatively uninformative, multiple such dumps – at, say, the location of each of a spate of bank robberies – can be cross-referenced in attempting to determine which individuals were present at all of the relevant places at all of the relevant times.[32] A second use of IMSI catchers, which follows directly on from this, is their use to block mobile phones (whether selectively or generally) – something which is often done, it seems, in prisons (as discussed in the following sections). A third, actual or hypothetical, use is to acquire metadata data related to the communications carried out by those phones. Finally, IMSI catchers can be used to intercept communications, acquiring not just the metadata relating to communications but their content, whether that be

[30] Though see note 25 above.

[31] See Shaun Nichols, 'US cops point at cell towers and say: Give us every phone number that's touched that mast' *The Register* (17 August 2017): "'In order to try to identify a suspect of a crime, the government may apply to a court for a warrant or order compelling us to provide a 'dump' of the phone numbers of all devices that connected to a specific cell tower or site during a given period of time," Verizon explained. "This tool is being used much more frequently by law enforcement." According to Verizon, tower dump requests were not particularly common in years past. In 2003, the carrier got a total of 3,200 dump warrants. By 2016, that number swelled to 14,630, and 2017 is on track for even more with 8,870 warrants halfway through the year.'

[32] See the discussion of such cases in Amanda Regan, 'Dumping the Probable Cause Requirement: Why the Supreme Court Should Decide Probable Cause is Not Necessary for Cell Tower Dumps' (2015) 43 *Hofstra Law Review* 1189.

what is said in the course of a telephone call or the contents (written or visual) of an SMS or other form of message.

Not all these uses are distinctive to IMSI catchers, of course. There is a significant body of law (very heavily used, of course) regarding the interception of communications and the acquisition of communications data. What is distinctive, however, is that such actions, if undertaken via an IMSI catcher, are examples of what have been described as 'direct' and 'unmediated' surveillance.[33] That is, they can be carried out by those who are in possession of an IMSI catcher, and are not reliant on the cooperation (whether voluntary or compelled) of telecommunications service providers, as is the case in 'mediated' or 'indirect' surveillance of the sort which is usually discussed, and about which much more is known.[34] The effect is that the safeguards which apply – including, perhaps, that the telecommunications providers might insist upon unambiguous compliance with the appropriate legal framework in order to inoculate themselves against potential liability – may be bypassed or elided by the use of IMSI catchers. Moreover, there is the possibility in the context of such unmediated surveillance, that interception will take place without the sort of written record normally produced by a process which implicates a multitude of parties, with their own interests (and own legal advice). And, though it is not the focus of the present work, this unmediated nature has implications not only for how IMSI catchers might be used, but also who might use them: the literature notes that though the technology evolves rapidly, the fundamentals of IMSI catchers is such that they might be made and made use of by a committed hobbyist, or other private parties which have no possibility of lawfully carrying out the interception of communications and so cannot compel the cooperation of telecommunications providers. And, of course, it is not only private parties who are so excluded by the legal framework: another possible use case is by foreign state actors in the United Kingdom, or by UK authorities in states where the standard mechanisms of mutual legal assistance are not available.

---

[33] Pell and Soghoian (n 28).

[34] Though it should be noted that the Investigatory Powers Act seems to foresee that interception authorised thereunder might be carried out either by a telecommunication provider or the entity to whom a warrant has been granted itself: see, eg, Investigatory Powers Act 2016, s 41(2) and (3): 'In giving effect to a warrant to which this section applies, the person to whom it is addressed… may (in addition to acting alone) act through, or together with, such other persons as the intercepting authority may require… to provide the authority with assistance in giving effect to the warrant.' This raises the possibility that in fact some of the interceptions which count towards the publicly available figures were in fact examples of unmediated surveillance, rather than the mediated surveillance with which the statutory powers seem usually to be associated. If this is the case, there would seem to be no way of knowing how many fall into each category.

3.3. The use of IMSI catchers in the UK

Before continuing, however, it is necessary to consider the extent of the problem to which we are here responding. Assuming we know how IMSI catchers *might* be used, we must ask also: *are* IMSI catchers used by public authorities in the United Kingdom? If so by which such authorities? Where and how? To what end? The answer is that there is a significant deficit of information, compounded by the relative paucity of oversight as compared to statutory powers of interception and acquisition of communications data, which were for many years overseen by the Interception of Communications Commissioner and are now overseen by the Investigatory Powers Commissioner created by the 2016 Act, discussed further below. Attempts to ascertain the extent of the use of IMSI catchers in the United Kingdom have been stymied by frequent recourse to 'neither confirm nor deny' responses to freedom of information requests.[35] In Scotland, however, requests have at times met with more success.[36] And even in England and Wales, where freedom of information has usually had little direct success, it has proven possible to identify the likely use of IMSI catchers by police forces by examining purchasing orders, which have often shown payments to Cellxion – the manufacturer of the devices and party to the patent dispute cited above.[37] And though the predictable NGOs and certain media outlets[38] have paid a certain amount of attention to the question of the use of IMSI catchers, there is little or no literature regarding their use. This creates an interesting contrast with the American

---

[35] See, eg, Freedom of Information Act 2000 (FOIA) Decision notice FS50660527 (8 June 2017) relating to an FOIA claim made to the Office of the Police & Crime Commissioner for Avon & Somerset, in which the Information Commissioner held that the OPCC was 'not obliged to confirm or deny whether the requested information was held'. In 2018, Privacy International, the NGO which has pursued a range of surveillance-related campaigns, reported that the Information Commissioner had held that the various police forces were not permitted to offer an NCND response to FOI requests relating to various categories of material – amongst them 'Marketing or promotional materials received by the police forces relating to IMSI catchers', legislation, and Codes of Practice' – but could continue to decline either to confirm or deny possessing other categories of material relating to the purchase and use of the devices: Privacy International, 'We can confirm that the police can no longer deny our freedom of information requests' (7 August 2018) available at https://privacyinternational.org/blog/2218/we-can-confirm-police-can-no-longer-deny-our-freedom-information-requests. Even in relation to material the possession of which must be either confirmed or denied, of course, refusal to disclose might be justified on one of the usual grounds.

[36] See, eg, 'Prisoners outwit £1.2m mobile phone blocking technology', *The Ferret* (25 May 2016) available at https://theferret.scot/IMSI catcher-trial-scottish-prison-service/, and describing material gleaned from a successful freedom of information request to the Scottish Prison Service.

[37] See Alon Aviram, 'Revealed: Bristol's police and mass mobile phone surveillance', *The Bristol Cable* (10 October 2016): 'Suspicions have been raised in the past that IMSI catchers are in use in the UK. These suspicions, until now, have focused on the Metropolitan Police's purchase and use of the technology. Now, the Cable can exclusively reveal that at least six other forces appear to have contracted for IMSI catchers, including Avon and Somerset (A&S) Constabulary.'

[38] Notably, non-traditional outlets such as Scotland's *The Ferret* and *The Bristol Cable* as well as technology-focused outlets such as *The Register*.

position, where talk of 'StingRays' – and in particular the implications therefore of the Fourth Amendment prohibition on unreasonable search and seizures – has been widespread in the law journals for several years already.[39] Though a number of written questions regarding the use by the police of IMSI catchers have been asked in the House of Commons, the responses so far given – though, as discussed below, in some ways revealing – have offered no tangible detail on these points.

3.4. The legal background

It is clear that there is at least some use of IMSI catchers in the UK and that, even if not used in their most intrusive fashion, there are potentially significant implications for individual rights associated with such use. This is most obviously the case with Article 8 rights to a private and family life, if one's presence in a particular place is being established as a derivative of knowledge of the presence there of their mobile phone, to say nothing of the retention (and possible disclosure) of any data acquired. That point will be considered further below. But a variety of other issues arise given that an IMSI catcher potentially permits for the monitoring of phones and, through them, individuals which are present in particular locations – at, say, a protest:

> This ability to identify secretly and accurately every member of a crowd, via their phone's identifier, goes beyond what government authorities traditionally have been able to accomplish. With normal visual surveillance, an officer might be able to identify a few

[39] See the material cited at notes 3 and 28 above as well as the following: Stephanie K Pell and Christopher Soghoian, 'A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us about How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities, (2013-14) 16 *Yale Journal of Law and Technology* 134; Jeremy H D'Amico, 'Cellphones, Stingrays, and Searches: An Inquiry into the Legality of Cellular Location Information, (2016) 70 *University of Miami Law Review* 1252; Ada Danelo, 'Legislative Solutions to Stingray Use: Regulating Cell Site Simulator Technology Post-Riley' (2016) 91 *Washington Law Review* 1355; Jason Norman, 'Taking the Sting out of the Stingray: The Dangers of Cell-Site Simulator Use and the Role of the Federal Communications Commission in Protecting Privacy & Security', (2016) 68 Fed. Comm. L.J. 139; Henry Bernstein, 'The Need for Fourth Amendment Protection from Government Use of Cell Site Simulators', (2016) 56 *Santa Clara Law Review* 177; Ryan C. Chapman, 'The Outer Limits: IMSI catchers, Technology, and the Future of the Fourth Amendment', (2017) 44 Pepp. L. Rev. 841; Coleman L. Torrans, 'How Did They Know That: Cell Site Simulators and the Secret Invasion of Privacy' (2017) 92 *Tulane Law Review* 519; Shawn Marie Boyne, 'Stingray Technology, The Exclusionary Rule, and the Future of Privacy: A Cautionary Tale' (2017) 119 *West Virginia Law Review* 915; Spencer McCandless, 'Stingray Confidential', (2017) 85 *George Washington Law Review* 993; Joshua Dansby, 'Stingrays', (2017) 74 Nat'l Law. Guild Rev. 72; Kristi Winner, 'From Historical Cell-Site Location Information to IMSI catchers: Why TriggerFish Devices Do Not Trigger Fourth Amendment Protection', (2017) 68 *Case Western Reserve Law Review* 243. These considerations may require revision in light of the decision of the US Supreme Court in *Carpenter v. United States* 585 U.S. ____ (2018).

> members of a rally with which he was already familiar, but to identify every single person within range seems to be beyond normal human observational abilities.[40]

Not only are the implications for individual rights of IMSI catchers (what rights are implicated, and to what extent) a function of how they are being used, but the question of their legal basis – whether one is required and whether it is available – will vary depending on the nature of such use (what, if any, data is being collected) and the identity of the party carrying it out. Below, I consider two broad scenarios: first, the use of IMSI catchers in relation to prisons and, second, their use outside that context.

It is necessary first, however, to explain how and why the question of legal authority varies according to the use to which IMSI catchers are put. That is, the basic rule of law position in England and Wales is that a requirement for legal authority exists only where the conduct being carried out is otherwise wrongful, in the sense of either changing the legal position of legal or natural persons or conflicting with some general prohibition found in the criminal law or the public or private law rights of an individual.[41] The relevant rules here are include, but are not necessarily limited to, the following. First, there exist specific provisions relevant to the point in the Wireless Telegraphy Act 2006 which makes it an offence both for a person to use wireless telegraphy apparatus except under a licence from OFCOM.[42] Given that an IMSI catcher is, by virtue of that Act's definitions, such apparatus, and does not appear to be the subject of any of the exemptions provided for by secondary legislation, this prohibition would seem to catch it and so make necessary the identification of some supervening legal authority. It is nevertheless necessary to considering further candidates for a relevant prohibition, not least because there is no reason to assume that state actors making use of the devices do not possess such licenses.

Another candidate is a provision which makes it an offence to use apparatus for the purpose of interfering with wireless telegraphy.[43] This latter prohibition applies whether or not the apparatus is 'wireless telegraphy apparatus', and whether or not regulations have been made

---

[40] Gus Hosein and Caroline Wilson Palow, 'Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques' (2013) 74 *Ohio State Law Journal* 1071, 1100.
[41] See *Entick v Carrington* (1765) 19 St Tr 1029 and *Malone v Commissioner of Police of the Metropolis (No 2)* [1979] Ch 344. For discussion, see the chapters by Endicott, Scott and Tomkins in Adam Tomkins and Paul Scott (eds), *Entick v Carrington: 250 Years of the Rule of Law* (Hart 2015).
[42] Wireless Telegraphy Act 2006, ss 8 and 35.
[43] WTA 2006, s 68.

regarding is sale and/or use under related provisions in the 2006 Act.[44] Any use of an IMSI catcher which is incompatible with one or the other of these rules will require supervening authority elsewhere in law. The key question which arises is therefore what counts as an 'interference' with wireless telegraphy for these purposes. The 2006 Act provides that '[f]or the purposes of this Act, wireless telegraphy is interfered with if the fulfilment of the purposes of the telegraphy is prejudiced… by an emission or reflection of electromagnetic energy'. Depending on the exact mechanism, therefore, it seems likely that blocking a mobile phone using an IMSI catcher represents such an interference, for to do so certainly prejudices the fulfilment of its purposes. On the other hand, using an IMSI catcher so as merely to 'catch' the IMSI of a device in range of it would not seem to prejudice the purpose of the telegraphy and so not represent an interference. Unless, therefore, it is prima facie prohibited by some other rule, such use of an IMSI catcher would not appear to require legal authority at all, regardless of the identity of the user. A second offence, however – found elsewhere in the Act – makes it an offence where a person – without lawful authority – uses 'wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addressee of a message (whether sent by means of wireless telegraphy or not) of which neither he nor a person on whose behalf he is acting is an intended recipient.'[45] Though this would suffice to create a requirement that legal authority exist for the use of an IMSI catcher (being 'wireless telegraphy apparatus') to that end, it is unclear where it would create one for the use of an IMSI catcher to merely catch IMSIs, which are not the content of the message, but are likely to be 'information as to the… addressee' if this latter term is understood expansively. And, finally but crucially, the 2006 Act does not bind the Crown,[46] and so while these rules form part of the relevant legal background, they will not necessarily inhibit all of the parties most likely to make use of IMSI catchers.

Relatedly, the Investigatory Powers Act 2016 re-enacts a number of relevant offences, including those of unlawful interception of a communication in the course of its transmission and the unlawful obtaining of communications data from a telecommunications operator.[47] That this latter offence does not apply to the acquisition of communications data generally – that is,

---

[44] WTA 2006, s 68(2). Such regulations can be made by OFCOM under section 54 of the Act: see, eg, the Wireless Telegraphy (Control of Interference from Apparatus) Regulations 2016 (SI 2016/426) which regulates the maximum intensity of electromagnetic disturbance caused by wireless telegraphy apparatus.

[45] WTA 2006, s 48, as amended by the IPA 2016.

[46] That is, there is no express provision in the Act which extends its application to the Crown, and it seems very unlikely that – in accordance with the general rule of statutory interpretation which applies in this area – such application is necessarily implied. For a recent consideration of the issue by the Supreme Court, see *R (Black) v Secretary of State for* Justice [2017] UKSC 81.

[47] IPA 2016, ss 3 and 11.

by means other than via a telecommunications operator – means that it cannot apply to the acquisition of an IMSI using an IMSI catcher, even if the IMSI is 'communications data' for the purposes of the Act; similarly, it does not apply generally, but only to those working within public authorities.[48] We need therefore note only the offence of unlawful interception,[49] to which these limitations do not apply: where an IMSI catcher is employed to that end it will, as with blocking of the signal, be necessary to point to supervening legislative authority which permits it. The picture, at this stage, therefore appears to be that only some of the possible uses outlined above are prima facie unlawful, and so require legal authority. The uncertain case is the use of IMSI catchers in their most ordinary function – to catch IMSIs – which is not caught by the 2016 Act offences and nor is it unambiguously caught by the relevant offences in the 2006 Act.

4. The law governing IMSI catchers in prisons

Some details of the use of IMSI catchers in prisons have found their way into the public domain, including a report of a trial carried out by the Scottish Prison Service. Several elements of the report are notable: one is the claim that the use of smartphones operating on 3G signals is more difficult to detect than their 2G predecessors due to the low power levels of output, and so required more sensitive detectors to be acquired by the SPS.[50] Given also the relatively high cost of smartphones (which were also less durable, and so less likely to survive, say, being thrown over a fence) prisoners who did not have access to their own were being tempted to 'rent' one from other prisoners, leading to 'debt and bullying amongst prisoner groups.'[51] Finally, the report noted that prisoners had developed 'innovative counter measures' which meant that the handset bypassed the false base station and connected directly to the public telecommunication network; it was later reported by another outlet that these countermeasures involved placing tin foil between the handset and the (visible to prisoners) IMSI catcher.[52] Though the body of public evidence is not large, it is therefore possible to be certain that such use is taking place in the specific prison context, and so to cross-reference this knowledge with the distinctive legal regime which applies in prisons. So, for example, the Investigatory Powers Act 2016 re-enacts the general prohibition on the interception of communications while simultaneously providing a

[48] IPA 2016, s 11.
[49] IPA 2016, s 3.
[50] Scottish Prison Service, 'Mobile Phone Signal Intervention End Project Report' (1 September 2015), 8: 'Prisoners outwit £1.2m mobile phone blocking technology' *The Ferret* (25 May 2016).
[51] Scottish Prison Service (n 50) 7.
[52] Gareth Corfield, 'Prisoners' 'innovative' anti-IMSI catcher defence was ... er, tinfoil' *The Register* (1 March 2017).

number of bases for lawful interception.[53] Amongst these is a provision which states that '[c]onduct taking place in a prison is authorised by this section if it is conduct in exercise of any power conferred by or under prison rules',[54] these being rules made under one of the statutes which govern conduct in prisons in England and Wales, Scotland, and Northern Ireland.[55] This will operate most effectively when those running prisons are in a position to intercept the communications in question via telecommunications providers: they will not be in said position if the communications are carried out with mobile phones obtained illicitly and used surreptitiously.[56]

Nevertheless, a number of provisions have been introduced and/or proposed so as to deal with the problem of illicit mobile phone use by prisoners.[57] In order to assist the enforcement of these rules, further provisions have been made in recent years which create exceptions to the general rules – found in the Wireless Telegraphy Act 2006 – that prohibit interference with wireless telegraphy. First, the Prisons (Interference with Wireless Telegraphy) Act 2012 – originally a Private Members' bill[58] – permits the 'appropriate national authority' to authorise the 'person in charge of a relevant institution to interfere with wireless telegraphy.'[59] Though this is a discretionary power, directions given under it are mandatory. The power to so authorise interference is limited to preventing the use of one of a number of types of device – 'a device capable of transmitting or receiving images, sounds or information by electronic communications (including a mobile telephone)', 'a component part of such a device' and 'an article designed or adapted for use with such a device (including any disk, film or other separate

---

53 IPA 2016, parts 1 and 2.
54 IPA 2016, section 49(1).
55 These being the Prison Act 1952, the Prisons (Scotland) Act 1989, and the Prison Act (Northern Ireland) 1953.
56 The Prison Rules provide that 'a prisoner shall not be permitted to communicate with any person outside the prison, or such person with him, except with the leave of the Secretary of State or as a privilege under' those Rules: Prison Rules 1999 (SI 1999/728), rule 34(1). A communication includes 'any communication from a prisoner to any other person transmitted by means of a telecommunications system'; a telecommunication system is 'any system (including the apparatus comprised in it) which exists for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.' Prison Rules 1999 (SI 1999/728), rule 2(1).
57 Prison Act 1952, s 40A. In the first place, a mobile telephone is, for the purposes of the Prison Act 1952, a 'list B' article. It is, that Act provides, an offence *inter alia* to bring, throw, or otherwise convey such an article into a prison, or to leave such an article 'in any place (whether inside or outside a prison) intending it to come into the possession of a prisoner': Prison Act 1952, s 40C. Section 40D makes it an offence to be in possession inside a prison of one of a number of items, including 'a device capable of transmitting or receiving images, sounds or information by electronic communications (including a mobile telephone)'.
58 A Ballot Bill sponsored by Sir Paul Beresford and Lord Laming.
59 Prisons (Interference with Wireless Telegraphy) Act 2012, s 1(1)

article on which images, sounds or information may be recorded)' – in a prison (or young offenders institution or secure training centre), or for 'detecting or investigating the use within the institution of such an item.'[60]

In relation to the latter use – detection and investigation – the Act provides that the interference which may be authorised thereunder is that 'for the collection of traffic data in relation to an electronic communication and… such an authorisation permits the retention, use and disclosure of that data.'[61] Given the definition of 'traffic data' in the Act,[62] this would appear to permit the collection not only of the metadata of particular communications, but also the IMSI of any mobile phone which might be used to send them, whether or not any are in fact sent. One point is worth noting: above, it was observed that it was not clear that the collection of an IMSI was an interference for the purpose of the Wireless Telegraphy Act and so it was not possible to be sure that legal authority was even required for the mere collection of IMSIs. The 2012 Act appears to make provision for interferences which do just that, suggesting a belief that authority was indeed required or – at a minimum – that there existed a desire to put the matter beyond doubt.[63] We see, then, that the Act appears to permit the first three of the uses of IMSI catchers noted above: catching IMSIs, blocking phones, and using IMSI catchers to acquire the metadata associated with particular communications. That this power was felt necessary suggests one of two things: either these acts could not otherwise be carried out, or they could be carried out only in a way which was impracticable or otherwise unacceptable.[64]

---

[60] P(IWT)A 2012, ss 1(2) and (3).

[61] P(IWT)A 2012, s 1(4).

[62] P(IWT)A 2012, s 4(4): traffic data is data 'which is comprised in, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted' and, *inter alia*, 'identifies or selects, or purports to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted.'

[63] The Act also makes provision for the retention and disclosure of information obtained under these provisions, the basic rule being that information must be destroyed within three months unless retention is authorised by the person in charge of the institution. Traffic data acquired on 'detection and investigation' grounds may be disclosed to only a limited group of persons unless its disclosure outside that audience has been authorised by the person in charge of the institution: Prisons (Interference with Wireless Telegraphy) Act 2012, s 3.

[64] Amongst the safeguards included in the 2012 Act are that details of the authorisation, and of the interferences which take place thereunder, are provided periodically to Ofcom: Prisons (Interference with Wireless Telegraphy) Act 2012, s 2. Memoranda of understanding between the relevant authorities (in England and Wales on one hand and Scotland on the other), Ofcom, and a number of mobile phone operators obtained by journalists using the Freedom of Information Act show a detailed agreement regarding the use of relevant equipment. Ofcom, according to one MoD 'will give advice to [the National Offender Management Service] on technical, coordination and interference issues [and] facilitate a dialogue between NOMS and the Mobile Network Operators… designed to ensure that appropriate procedures are put in place and followed, in the event of interference arising beyond the prison perimeter

Following logically from the 2012 Act is the power in the Serious Crime Act 2015 to permit the making of regulations which confer 'power on a court to make a telecommunications restriction order', being 'an order requiring a communications provider to take whatever action the order specifies for the purpose of preventing or restricting the use of communication devices by persons detained in custodial institutions.'[65] Two sets of regulations have been made under this power, one each in relation to Scotland and to England and Wales.[66] The latter permit the county court to make a telecommunications restriction order where it is 'satisfied that a communication device identified in the order is inside a custodial institution' and 'has no reason to think that the device is in the possession of a person who has authorisation to possess it.'[67] The explanatory memorandum to the regulations explain that a TRO 'will require Mobile Network Operators (MNOs) to disconnect specified, unauthorised mobile phones without the need to first take physical possession of the device or attribute its use to individuals' and that '[t]he number of mobile phones specified in the application will depend on how many mobile phones are identified as being in use in the relevant custodial institution.'[68] This makes clear, it would seem, that it is anticipated that TROs will be used in situations where the authorities are aware of the presence of phones in prisons, and have enough information about the phones in question to be able to require the operators to block them. It seems highly likely that one of – perhaps the only – way in which they will acquire that knowledge is via the use of IMSI catchers: the explanatory notes say only, somewhat enigmatically, that applicants 'will properly test and calibrate the technology they use to identify unauthorised mobile phone in prisons, making sure only unauthorised phones in use in custodial institutions are identified and progressed through the… process.'[69] And a block put in place in this way is mediated (by the MNO) rather than unmediated; once and for all rather than only until the phone in question is out of the device's range.

---

that may be attributable to the use of the Equipment, in line with its statutory duties to manage the radio spectrum.' Ministry of Justice, Ofcom, and four Mobile Network Operators, 'Memorandum of Understanding on the use of radio frequency interfering equipment within prisons' (nd) [5].

[65] Serious Crime Act 2015, s 80. Amongst other things, regulations so made must, the Act provides, specify 'who may apply for telecommunications restriction orders', 'make provision conferring rights on persons to make representations', 'specify the matters about which the court must be satisfied if it is to make an order' and 'make provision about the duration of orders'.

[66] Telecommunications Restriction Orders (Custodial Institutions) (Scotland) Regulations 2017 (SI 2017/423); Telecommunications Restriction Orders (Custodial Institutions) (England and Wales) Regulations 2016 (SI 2016/8303).

[67] SI 2016/8303, reg 3.

[68] Explanatory Memorandum to the Telecommunications Restriction Orders (Custodial Institutions) (England And Wales) Regulations 2016, [7.8].

[69] Explanatory Memorandum (n 68) [7.12].

Finally, the Prisons and Courts Bill, introduced in early 2017, contained a provision which would have amended the Prisons (Interference with Wireless Telegraphy) Act 2012 so as to permit the Secretary of State to 'authorise a public communications provider to interfere with wireless telegraphy', alongside the existing possibility of interference by the person in charge of the institution.[70] The permitted purposes of such an interference would again have been 'preventing the use within a relevant institution in England and Wales of' mobile phones and related devices, or 'detecting or investigating the use within a relevant institution in England and Wales of such an item.'[71] The Bill was aborted as a result of the calling of the early general election, but the key provision was later revived as a private members bill,[72] passed in late 2018 and – at the time of writing – awaiting Royal Assent. What gap, exactly, the provision is intended to fill is not entirely clear. The original delegated powers memorandum noted that the provision's purpose was to permit PCPs to 'operate independently to deploy new technologies to disrupt the use of illegally held mobile phones in custody.'[73] A related impact assessment noted that the Bill would 'provide clearer lines of accountability to allow PCPs to act more independently where necessary and appropriate and will ensure that adequate safeguards apply where the PCP is effecting interference.'[74] Neither of these seems to get at the heart of the matter: rather, it appears that the key novelty is the ability to give general directions to mobile phone operators to use their own equipment to carry out the blocking of phones, and to have them do so more or less automatically, without the need for individual prisons to own and operate the relevant equipment. And so, even in the context of prisons, where the secrecy surrounding the use of IMSI catchers is not quite so profound as it is elsewhere, it is difficult to fully grasp the effect and significance of the relevant law, notwithstanding that it is – on its face – clear and accessible. Outside the prison context, that difficulty is much greater.

5. The legal basis of IMSI catchers in a non-prison context

In the non-prison context, the legal basis of the use of IMSI catchers is less certain.[75] This itself is hardly unusual: as noted above, much of the law of investigatory powers was until very

[70] Prisons and Courts Bill 2016-17, Bill 145, clause 21.
[71] Prisons and Courts Bill (n 70) clause 21.
[72] Prisons (Interference with Wireless Telegraphy) Bill 2017-19.
[73] Ministry of Justice, Delegated Powers Memorandum for the Prisons and Courts Bill (nd), [36].
[74] Ministry of Justice, Prisons and Courts Bill - Overarching Impact Assessment (22 February 2017) [41].
[75] See Anderson (n 7) [12.8]: 'It has become increasingly apparent during the course of this Review that a range of techniques and methods is utilised (in particular by the security and intelligence agencies). Some

recently 'hidden in plain sight', it being in many cases impossible to know what statutory powers were being used to carry out what sort of actions, and if the authorities are unwilling to openly acknowledge the use of IMSI catchers, they are hardly going to undermine that position by giving a full and frank account of what the legal position would be in the hypothetical event that they did so. And yet in the case of IMSI catchers, the problems endemic to the law of surveillance are exacerbated. That is, as made clear in preceding sections, IMSI catchers can be used in a variety of ways, of greater or lesser intrusiveness. But though the device is or might be the same in each case, the simple act of using it in different ways will shift it from one legal regime to another; even in the era of the rationalisation of investigatory powers by the 2016 Act, it may result in the legal basis moving from one part of that Act to another. And so, without knowing how the device is in fact used, it is difficult to know what is the applicable legal regime, and what are the key questions which determine whether any specific use is or is not lawful. Moreover, IMSI catchers permit – we have noted above – undifferentiated and unmediated surveillance, limited only by the physical location of the (portable) device itself.

A series of questions about IMSI catchers in Parliament, however, have elicited responses – always in identical terms – which offer some limited insight into the relevant authorities' understanding of the legal position, though without in fact answering the questions posed.[76] The key sections of those answers are as follows:

> Investigative activity by public authorities involving interference with property or wireless telegraphy is regulated by the Police Act 1997 and the Intelligence Services Act 1994, which set out the high level of authorisation required before law enforcement or the security and intelligence agencies can undertake such activity. The covert surveillance and property interference code of practice provides guidance on the use of these powers.
>
> In addition, the Investigatory Powers Act 2016 will regulate the interference with equipment for the purpose of obtaining communications, equipment data or any other

---

of these intrusive practices do not find clear and explicit basis in legislation, other than general powers in SSA 1989 and ISA 1994. They include… the use, such as there is, of other surveillance instruments available to the public, such as IMSI catchers.' These remarks of course predate the enactment of the Investigatory Powers Act 2016, discussed further below.

[76] Written questions 121464, 121465 and 121466. All three questions were asked on 8 January 2018 by Thangam Debbonaire MP and answered on 11 January 2018 by Nick Hurd MP, Minister of State in the Home Office.

> information. These provisions will come into force later this year, and further guidance will be provided in a statutory code of practice.[77]

Several insights can be gleaned from this answer. The first, and most important, is that the authorities appear to view at least some uses of IMSI catchers as representing a form of property interference. That is what the 1994 and 1997 Acts have in common, containing the provisions which – we now know – allow the security and intelligence agencies and police respectively to carry out 'computer network exploitation' – what is now called 'equipment interference' and is more colloquially described as hacking.[78] The reference to the EI provisions of the 2016 Act, to which we will return below, confirms the point. One question which this prompts, however, is whether the general nature of the interference which an IMSI catcher carries out can be permitted under the relevant legislation. That is, it is clear that an IMSI catcher interferes with those phones which come into its range generally, rather than being targeted at specific phones. This makes sense: if at least part of the point of using the device is to determine how many, if any phones, exist in a given area – as in a prison – then by definition it will not, because it cannot, be known in advance what property is going to be interfered with. But do the relevant provisions of the legislation identified permit interferences of such a broad sort? The answer to that would seem to depend on the question discussed above: whether the interference takes place at the point at which the mobile phone connects to the IMSI catcher (and so the latter becomes aware of the former's existence and so presence etc) or whether it comes only when some further event takes place – the blocking of the phone, say, or the acquisition of data (whether content or 'communications data') from that phone (a question of further relevance in the era of the Investigatory Powers Act). As a matter of 'domestic' law, the answer appears to be the latter: because there is no prima facie prohibition on use which simply results in a mobile phone connecting to the device, then there is no requirement of legal authority for such use. There is therefore no need to concern ourselves with the quality of such authority, which becomes an issue only at the point at which ban interference takes place – whether blocking (contrary to the terms of the 2006 Act) or the interception of communications or acquisition of metadata (both contrary to prohibitions found in the 2016 Act). That conclusion is though subject to modification in light of the provision of the Wireless Telegraphy Act discussed above – which makes it offence to use apparatus 'with intent to obtain information as to the contents,

[77] ibid.
[78] Scott (n 1).

sender or addressee of a message' and may therefore cover the use of IMSI catchers if an IMSI is 'information as to the… addressee of a message'.

For those acts which do require legal authority, the existence of a bare legal basis does not itself, however, resolve the problem of the generality of the effect of IMSI catchers. It was noted above that surveillance carried out by means of an IMSI catcher is unmediated, not relying upon the involvement of telecommunication providers. It is also, we must emphasise here, (actually or potentially) undifferentiated, meaning that though IMSI catchers can only have effect where they are physically located (though reports of planes carrying the devices of course undermine that limitation, and the devices are entirely portable), the correlative is that they impact upon (to use a suitably neutral term) *all* phones and similar devices within the affected area. So, to be clear: an authorisation under the 1994 Act or 1997 Act may, where it permits the use of an IMSI catcher, result in an interference with the rights of persons who are not and who cannot be identified in those authorisations but rather all those (or all devices) in geographic range of the device. But interception warrants have always been available also on what is described as a 'thematic' basis, where their target is identified not as a particular person but as an 'association or combination of persons'.[79] The Investigatory Powers Tribunal, which rules on the legality of the uses of most investigatory powers, has had occasion to consider the lawfulness of 'thematic' warrants under section 5 of the 1994 Act.[80] It held, contrary to normal canons of interpretation, that a warrant authorising interference with property did not need to specifically identify the property in question.[81] Rather, '[t]he property should be so defined, whether by reference to persons or a group or category of persons, that the extent of the reasonably foreseeable interference caused by the authorisation of CNE in relation to the actions and property specified in the warrant can be addressed.'[82] Crucially for present purposes, amongst the submissions made to – and accepted by – the Tribunal was the claim that a warrant authorising interference with 'all mobile phones in Birmingham' would be 'sufficiently specified', even if 'save in an exceptional national emergency' it would be unlikely that such a warrant would be 'either consistent with necessity or proportionality or with [the Government Communication

[79] This possibility is now given effect more explicitly than in the past. The 2016 Act provides that a so-called 'targeted' warrant relates to either 'a particular person or organisation' or 'a single set of premises', but adds that a targeted warrant may relate also to 'a group of persons who share a common purpose or who carry on, or may carry on, a particular activity' or 'more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation: IPA 2016, s 17.

[80] *Privacy International v The Secretary of State for Foreign and Commonwealth Affairs and the Government Communications Headquarters* [2016] UKIP Trib 14_85-CH.

[81] See the discussion in Scott (n 1).

[82] [2016] UKIP Trib 14_85-CH, [38].

Headquarters] statutory obligations.'[83] It seems, therefore, that 'all mobile phones being used in [the location of some protest]' would be similarly acceptable from the point of view of specification, and would in fact be much more likely to meet the requirements of necessity and proportionality.

The equivalent provision within the Police Act 1997 is section 92, which provides that '[n]o entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by an authorisation having effect under this Part.' An authorisation may – subject to requirements of necessity and proportionality – authorise 'the taking of such action, in respect of such property in the relevant area' as the authorising officer 'may specify', or 'the taking of such action in the relevant area as he may specify, in respect of wireless telegraphy.'[84] 'Relevant area' here simply means the area covered by the police authority to which the authorising office belongs.[85] On its face, therefore, there is sufficient similarity between this provision and the terms of section 5 of the Intelligence Services Act 1994 that what was decided in relation to the latter would seem equally capable of applying to the former, allowing – that is – the 1997 Act too to ground the issue of 'thematic' authorisations. And yet the terms in which the IPT's decision was couched suggest that may not in fact be the case. The basic interpretive rules is what is known to constitutional lawyers as the 'principle of legality', whereby Parliament is perfectly entitled to authorise interferences with fundamental rights (such as, here, the right to property) but must do so explicitly, it being the case that 'general' or 'ambiguous' terms might pass through the Parliamentary process without their implications for particular rights being appreciated, and the relevant 'political cost' therefore being paid.[86] In its consideration of the 1994 Act, the IPT did not give effect to this principle and rejected the claim that the 'abhorrence of general warrants issued without express statutory sanction' which was such a prominent element of eighteenth century public law was 'a useful or permissible aid to construction of an express statutory power given to a Service, one of whose principal functions is to further the interests of UK national security, with particular reference to defence and foreign policy.'[87]

Its approach to interpretation was therefore straightforward: 'The words', it said, 'should be given their natural meaning in the context in which they are set.'[88] It is not clear here exactly what the basis of this decision is: if the principle of legality has no application to the facts, or if

[83] [2016] UKIP Trib 14_85-CH, [36].
[84] Police Act 1997, s 93(1).
[85] PA 1997, s 93(6).
[86] *R v Secretary of State for the Home Department, ex parte Simms* [2000] 2 AC 115, 131.
[87] [2016] UKIP Trib 14_85-CH, [37].
[88] [2016] UKIP Trib 14_85-CH, [37].

the Tribunal was, in effect, asserting an exception to the general rule in the case of bodies responsible for national security. If the latter, then this is surprising, and incompatible with the approach which has been taken by the Supreme Court in recent years.[89] It is nevertheless significant from the point of view of the use of IMSI catchers by the police under the Police Act – which, as the Parliamentary answers quoted above seem to suggest, was the relevant test. That is, however one conceptualises the role of the police, it is clearly less sensitive than is that of national security – this we see throughout the constitutional order, where the most intrusive powers are afforded to the SIAs to protect the interests of national security and related ends, and the police and other public authorities permitted only to carry out lesser intrusions. If, therefore, the principle of legality is caveated by the needs of national security, then there is no reason to apply the same interpretive approach to the 1997 Act's power of property interference. It the context of the this latter, 'specify' should – it is submitted – be read as imposing more a more demanding requirement than is created by the very low threshold for adequate specification applied in the context of ISA warrants, one which – again, it is submitted – would rule out a merely geographical specification of the sort described above, used to interfere not only with property belonging to people who are not named, but with that belonging to people whom those seeking, and those granting, such authorisations cannot name.

The Parliamentary answers noted above reference also the Investigatory Powers Act 2016, the terms of which must now be taken into account. The Act implements – amongst other things – regimes for the interception of communications, the acquisition of communications data and equipment interference, all of which exits in both 'targeted' and 'bulk' forms. The powers in the 1994 and 1997 Acts persist, though their use is now subject to restriction. In the case of the former, the rules is that the SIAs may not 'for the purpose of obtaining communications, private information or equipment data, engage in conduct which could be authorised by an equipment interference warrant except under the authority of such a warrant if (a) the intelligence service considers that the conduct would (unless done under lawful authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences), and (b) there is a British Islands connection.'[90] The effect is that where there is a British Islands connection, the 1994 Act can no longer be used to ground the use of IMSI catchers if the intention of doing so is to also acquire communications, private information or equipment data. The implications of this must be unpacked. First of all, is an IMSI equipment data? Does one

[89] See, eg, *HM Treasury v Ahmed* [2010] UKSC 2.
[90] IPA 2016, s 13.

need to 'acquire' an IMSI in order to block a mobile phone? If the answer to both these questions is 'yes', then the 1994 and 1997 Acts can no longer be used to permit that blocking. If not, the legal regime has become (further) fragmented, so that the 1994 and 1997 Acts can permit the use of IMSI catchers to block mobile phones, but not other uses, which must instead take place under the 2016 Act. Note, though, the point made above about the use of IMSI catchers abroad, where the UK authorities have no sway over telecommunications providers (or, if they do, no desire to make those providers aware of their activities). In such cases, the fact that there is no British Island connection means that the 1994 Act – in practice, not the section 5 power but its section 7 counterpart – can still be used for the purpose of acquiring IMSIs (if they are equipment data) and the content of, and metadata associated with, communications.

Though it proves nothing decisively, the mention of the 2016 Act within the Parliamentary answers therefore implies that IMSI catchers are, or might in future, be used for those purposes which can no longer be grounded in the 1994 and 1997 Acts. And, further, in considering the relevant terms of the 2016 Act, we can restrict ourselves to 'targeted' equipment interference, the 'bulk' variety being limited to the acquisition of 'overseas-related' information, whether than be communications sent from or to individuals who are outside the British Islands or information about such persons. Whatever is the case, the point about the undifferentiated nature of the surveillance effected by an IMSI catcher (and necessarily thematic nature of a warrant permitting its use) holds true. A targeted equipment interference warrant permits interference for the purposes of communications, equipment data, or 'any other information'.[91] It can be granted where necessary and proportionate on one of a number of grounds, including 'for the purpose of preventing or detecting serious crime' (with the process differing depending on whether granted to the intelligence services or the police); the availability of such warrants is to that extent no greater than was that of warrants/authorisations under the 1994 and 1997 Acts. Though a warrant is 'targeted', it is now made explicit that this does not imply that specific persons be named within the warrant: indeed, the 2016 Act provides that a targeted EI warrant may relate, amongst other things, to 'equipment in a particular location' or even 'equipment in more than one location, where the interference is for the purpose of a single investigation or operation.' Assuming the other requirements are met, therefore, there is no doubt that it would be lawful to grant a targeted EI warrant which permitted interference with all equipment (ie, mobile phones) in Pentonville prison, or even all equipment in *all* prisons, where it was part of a single operation aimed, say, at cracking down on the illicit use of mobile phones by prisoners. It could also be used in a variety of other 'thematic' contexts and though the carrying out of equipment interference is restricted to a limited set of grounds, amongst these is 'preventing or detecting serious crime' which is defined to mean crime where either 'the offence, or one of the

[91] IPA 2016, s 99.

offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18… and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more' or 'the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose'.[92] This is not a high bar.

Finally, the responses to the various Parliamentary questions have noted that 'Ownership and operation of such devices by police forces and other public authorities is an operational matter for them.'[93] This would be an acceptable response were there not such a pervasive unwillingness on the part of the police to acknowledge the mere fact of such ownership and operation. Leaving aside the special context of prisons, these devices have a very broad effect and – depending on how they are used – potentially very significant implications not only for privacy but also for freedom of expression and assembly. These implications cannot be discussed nor challenged if the use of the technology remains secret. We see again in this context that though the law is now clearer than was the case even a few years ago, the factual uncertainty as to what IMSI catchers are used to do, and how they do it, makes analysis of the actual and possible legality of surveillance in the contemporary United Kingdom very difficult. This suggests once more that the rule of law will not be achieved within the surveillance state until not a factual transparency comparable with the new legal transparency has been achieved. Until then, too much will have to be taken on trust. And, of course, what is true of IMSI catchers applies a fortiori to other surveillance technology of which we ae as yet unaware, and of which we perhaps cannot even conceive.

6. Article 8 of the European Convention on Human Rights

There was discussed above the difficulty of ascertaining precisely what are the rules of 'domestic' law with which the various uses of IMSI catchers are incompatible, such that they will require legal authority. The same question arises in the context of the Convention on Human Rights, the most relevant provision of which will be Article 8, which protects the right to a private and family life. That is, the first point to consider is when and where Article 8 is even engaged. It certainly will be where communications or the associated metadata are acquired using an IMSI

[92] IPA 2016, s 263.
[93] Hurd (n 76).

catcher,[94] the Strasbourg court being generally uninterested in the specific method of surveillance. What of circumstances where there is some purportedly lesser interference? Where the device is used to block or simply to collect the IMSI of a phone, without then using that information in order to collect any content or metadata? It is difficult to say. In the first case, the claim is a tenuous one: though Article 8 refers not only to a person's private and family life but also to 'his home and his correspondence', blocking mobile phones does not interfere with his correspondence and can only be brought within the wider concept with some difficulty, by arguing – perhaps – that blocking mobile phone calls using an IMSI catcher acts to prevent a person communicating with his family. In the second, an IMSI is simply a number, which though it can used to acquire information about the subscriber to the phone, on its own tells us nothing about that person – not even his or her identity – and may therefore not be an aspect of 'private and family life' even where that concept is widely defined.

Nevertheless, the Court of Human Rights has been willing to look at the reality of the situation rather than draw legalistic distinctions in this area. In *Uzun v Germany*, the Court rejected the argument that there had been no compilation of data about a person when they were tracked via GPS because 'the GPS receiver had been built into an object (a car) belonging to a third person (the applicant's accomplice).'[95] In that case, it noted that 'investigating authorities clearly intended to obtain information on the movements of both the applicant and his accomplice' and that they 'systematically collected and stored data determining, in the circumstances, the applicant's whereabouts and movements in the public sphere.'[96] Therefore, though it accepted that 'GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings' it nevertheless concluded that there had been an interference.[97] Similarly, it is clear from this case, and from others,[98] that the fact that a person is in public does not mean that he or she can have no reasonable expectation of privacy such that there can be no interference with his or her Article 8 rights. If, of course, an IMSI catcher were

[94] See, eg, *Malone v United Kingdom* (1992) 14 EHRR 657, which though it suggests that the acquisition of metadata is, from the perspective of Article 8, less intrusive than is the interception of the content of a communication, it is nevertheless an interference for Article 8 purposes, and *Big Brother Watch v United Kingdom* (58170/13) in which the lesser safeguards associated with 'related communications data' acquired via bulk interception under RIPA were central to the Court's decision that the regime of bulk interception violated Article 8 of the Convention.
[95] *Uzun v Germany* (2011) 53 EHRR 24.
[96] (2011) 53 EHRR 24, [51].
[97] (2011) 53 EHRR 24, [52].
[98] See, eg, *Peck v United Kingdom* (2003) 36 EHRR 41.

used to determine who was in a particular home – something which would normally require a surveillance authorisation[99] – that would seem to count conclusively in favour of the claim that an Article 8 interference is taking place.

The *Uzun* case, however, is only a helpful analogy for some uses of IMSI catchers. It would seem analogous to the use of such a device in order to acquire the details of a particular person, where the phone is being used as a proxy in the manner in which the GPS device was in *Uzun*. If, alternatively, it is being used to identify the phones which are present in a given location with a view to later matching those devices to people, it may be that there is no interference, which will instead happen – if at all – at that second stage. On balance, therefore, it is likely that some uses of an IMSI catcher will not count as interferences with Article 8, and so will not require justification according to the criteria there offered.[100] For those interferences which do require such justification, the usual criteria will apply. For the most part, these should be capable of being met by the use of IMSI catchers now that the legal basis has been rationalised and now that the law is accompanied by a Code of Practice of the sort which have long existed in the context of interception of communications and which is of considerable assistance in bridging the gap between the bare statutory language of the law and the *Weber* requirements which the Strasbourg Court enforces in the context of secret surveillance.[101] The question of foreseeability is the most likely source of difficulty: given how little is in the public domain about the devices and their possible uses, it seems unreasonable to expect the ordinary person to reason from broad statutory powers to, for example, the collection of IMSIs by the state. Because, however, those uses least likely to be foreseeable are also those least likely to constitute an interference for Article 8 purposes, the Convention is not necessarily an insurmountable obstacle to the use of the IMSI catchers considered in the round.

7. Oversight

Unsurprisingly in light of the foregoing, there is no specific oversight of the use of IMSI catchers in the United Kingdom. There has been, however, limited and non-statutory oversight of their use in prisons in England and Wales by the Interception of Communications Commissioner

[99] RIPA 2000, part II.
[100] If this conclusion is wrong, then one question will be whether any interference grounded upon the relevant provisions of the Police Act 1997 can be 'in accordance with the law' given that such provision does not – for reasons given above – seem capable of permitting 'thematic' warrants, and so such use cannot, by definition, be 'in accordance with the law'.
[101] *Weber and Saravia v Germany* (2008) 46 EHRR SE5.

('IOCCo') – oversight which was taken over (now on a statutory basis) by the Investigatory Powers Commissioner when he replaced IOCCo (as well as the Intelligence Services Commissioner) following the enactment of the Investigatory Powers Act 2016. A statement by the IOCCo in early 2017 confirmed that the Commissioner had received 'a formal letter from the Prime Minister asking him to provide oversight of a non-statutory basis of IMSI catchers in prisons within England and Wales, until the Investigatory Powers Commission has been set up.'[102] It further stated that the Commissioner did not 'currently plan to produce a separate report about this subject' but that it was 'anticipated the subject will be included within the Commissioner's 2016 Annual Report, which is due to be released later this year.'[103] When that report was in fact released, however, it made no specific mention of the use of IMSI catchers, with the report focussing instead upon the interception of communications in prisons,[104] and no attempt to distinguish between the different methods by which such interference was or is carried out. This suggests either that IMSI catchers were not being used for interception, or – more likely – that they were, but that such use was bundled together with more traditional interception. No oversight took place at that time in relation to the use of the devices in Scotland.

The IPA 2016 charges the new Investigatory Powers Commissioner with 'the exercise by public authorities of statutory functions' which relate to, inter alia, the interception of communications or the acquisition of communications data. This will include such interception within prisons. The Commissioner is also now charged, however, with keeping under review 'the exercise of functions by virtue of section 80 of the Serious Crime Act 2015' (the power discussed above regarding the prevention or restriction of use of communication devices by prisoners) and the exercise of functions under the Prisons (Interference with Wireless Telegraphy) Act 2012.[105] Both of these enactments extend, in the relevant provisions, to Scotland, and there appears to be nothing within the 2016 Act which would perpetuate the unhelpful geographic distinction of the status quo ante. Though the fact of oversight is, of course, welcome, not least because it confirms that the use of IMSI catchers would not otherwise be caught by the statutory functions of IOCCO (or, indeed, his fellow Commissioners) this situation retains certain anomalies. The first is the arbitrary nature of the oversight which exists. This is so not only from a geographic point of view: though Scotland has now been added, Northern Ireland is not within the IPC's

[102] 'Scrutiny over phone snooping tech won't extend to Scotland' *The Ferret* (9 March 2017).
[103] ibid.
[104] The Rt Hon. Sir Stanley Burnton, *Report of the Interception of Communications Commissioner Annual Report for 2016*, (HC 2017-19, 297), 50-3.
[105] IPA 2016, s 229.

remit in this area. The oversight may also be arbitrary in applying to the use of IMSI catchers only in prisons. To know for sure whether this is the case, however, involves answering the same questions which have been the source of the uncertainties considered above: who is using such devices, and how. That is, if the use of IMSI catchers outside of prisons is distinct from its use in relation to prisons, such that the former – unlike the latter – falls within the statutory oversight of one Commissioner or another, or (now) the Investigatory Powers Commissioner, then this anomaly does not arise. Unfortunately, as with many of these issues, there is no way to know. What is notable, however, is that even where there was non-statutory oversight – in the form of the 2016 report by IOCCO – the devices were not named and their use was not directly remarked upon. If that continues even into the era of statutory oversight, the suspicion that in relation to IMSI catchers secrecy is to be maintained at (almost) all costs will be once more strengthened.

8. Conclusion

The basic trajectory of the law which governs surveillance state in recent years has been one of rationalisation: of taking powers out of the shadows in which they had been created and grown up, and placing them on a new footing, one which is more explicit and more transparent, even if the opportunity was in many cases taken to give powers a form as broad as, if not broader than, the widest possible interpretation of the prior position. The effect, for the most part, has been a significant improvement – the possibility of understanding of what the state might lawfully do is this domain is greater now than it has ever been. The question of IMSI catchers, however, demonstrates the limitations of an approach which starts from powers and reasons out from there. IMSI catchers have a number of capabilities, which cut across the neat divisions of investigatory powers as found, now, in the 2016 Act. We know that they exist and we know that they are used in prisons – and probably outside of them – but the we do not know enough about how they are used to be sure that the law as it exists adequately regulates these various uses. At the flick of a switch, we might move from a use which is only minimally intrusive (and so subject to commensurately few, relatively weak, legal safeguards) to one which is much more intrusive, and in relation to which the safeguards which apply are much more numerous and stricter. The potential for abuse is readily apparent, and is magnified by the fact that there are – in this picture – no telecommunications providers which might perform a gate-keeping function, out of concern for their own legal position if not that of their customers.

More than anything, however, IMSI catchers (which are, let us remember, hardly cutting-edge technology) are a case study in how secrecy as to factual matters will be the new battleground in attempts to subject the surveillance state to the rule of law. To know the content of the law does not suffice. It is, of course, entirely reasonable for public authorities to try to keep secret their capabilities and the specific technical methods by which they are carried out. To the claim in this article, they would no doubt respond that the law is clear and that they act within it. Perhaps. But the prevailing atmosphere of secrecy – the non-disclosure agreements and the resistance to attempts to use the freedom of information acts to shed light on the equipment various facets of the state possess, whether through Freedom of Information Act requests or parliamentary processes – makes it highly unlikely that these issues will ever be tested by any judicial actor: who will challenge the use of IMSI catchers if all that is ever known is the bare fact that some police forces possess them? The IPA 2016 makes provision for a Technology Advisory Panel to advise the Investigatory Powers Commissioner (the new oversight actor in this area) on 'the impact of changing technology on the exercise of investigatory powers whose exercise is subject to review by the Commissioner' and 'the availability and development of techniques to use such powers while minimising interference with privacy'.[106] While better than nothing, the advice in question would be of more use to the public at large, who could then be confident that the veil of secrecy which prevails here was something more than a convenient way of ensuring that technological developments were being exploited to their full extent but without needing to pay any associated political, or legal, price for doing so.

[106] IPA 2016, s 246.