IMSI-CATCHERS

"Law enforcement's worst kept secret"

A cause for legal and ethical concern

THE BRISTOL CABLE

A Bristol Cable briefing 2017/18

The Bristol Cable was founded in 2014. It is the UK's only citywide media co-operative, specialising in investigative and campaigning journalism and media training. It is based in Bristol and has over 1900 members. Bristol Cable investigations have been cited in the Houses of Parliament and co-published across dozens of national and regional titles. It is an accredited member of the Global Investigative Journalism Network.

thebristolcable.org @thebristolcable

Alon Aviram *Author* is an operations and media co-ordinator at the Bristol Cable. His 2016 investigation into IMSI-catchers revealed that British police forces had purchased the technology.

Silkie Carlo *Contributor* is the senior advocacy officer at Liberty. She leads Liberty's programme on Technology and Human Rights, advocating for the protection of rights in areas including state surveillance, new policing technologies, uses of big data, artificial intelligence and free expression online.

Angela Patrick *Contributor* is a barrister at Doughty Street Chambers, where she specialises in human rights and public law cases. Until 2016, she was Director of Human Rights at JUSTICE, where she led its work on national security, surveillance and the Investigatory Powers Act 2016.

Contact Alon Aviram, *Operations and media co-ordinator, the Bristol Cable*
Email: imsi@thebristolcable.org **Direct line:** 07533718547

Introduction

International Mobile Subscriber Identity-catchers (IMSI-catchers) comprise a range of powerful indiscriminate mobile phone surveillance technologies, which allow thousands of individual mobile phones to be spied upon.

To date, the Home Office and individual police forces have pursued a policy which will neither confirm or deny the possession or use of IMSI-catchers. Public authorities and ministers have consistently refused to declare whether police or other agencies possess or operate the technology, despite mounting evidence. Following the Snowden revelations, a number of bulk data retention techniques were avowed during litigation in the Investigatory Powers Tribunal (IPT). The Government called the Investigatory Powers Act 2016 (IPA) a step away from the historical lack of openness. Yet, continued stonewalling on IMSI-catchers has stifled public debate, prevented democratic oversight, and gravely undermined the principle of policing by consent.

There is an urgent need for the Home Office and police to disclose to Parliament the following:

1. The legal basis and governing procedures for IMSI-catcher deployment and data processing and retention.
2. A statistical overview of all historic IMSI-catcher deployments by UK authorities.
3. The public authorities that currently own or operate IMSI-catchers.

The time has come for a rigorous debate over the use of IMSI-catchers in the UK to assess whether benefits from such surveillance technology are proportionate to the collateral violations of privacy.

This briefing has been co-ordinated by the Bristol Cable, with two contributing authors providing specific analysis. The contravention of civil liberties by IMSI-catchers is outlined by Silkie Carlo, Senior Advocacy Officer for Liberty. Angela Patrick, Barrister at Doughty Street Chambers, explains why the legal basis for the roll-out of IMSI-catchers is far from clear.

What we know so far

Nine UK constabularies are known to have purchased IMSI-catchers in recent years. This information only came to light after police procurement data and documents were analysed by the Bristol Cable.[1] The investigation evidenced that constabularies had spent hundreds of thousands of pounds (over £1m by the Metropolitan police alone) on IMSI-catchers, and that they were using an acronym - CCDC (covert communications data capture) - to disguise transactions.

To date, the Metropolitan, Avon and Somerset, South Yorkshire, West Midlands, Warwickshire, West Mercia, Staffordshire, Essex and Kent constabularies are known to have purchased IMSI-catchers. Despite evidence, these forces continue to neither confirm or deny that they own or operate IMSI-catchers. The only public authority in the UK that has admitted to using IMSI-catchers is the Scottish Prison Service, which via the Freedom of Information Act, disclosed to the Ferret magazine that it trialled the technology in prisons in Scotland to block smuggled mobile phones.[2]

As IMSI-catchers are likely to become more capable, cheaper and more portable with time, the frequency of their use by law enforcement agencies is likely to increase, and the privacy implications will increase in tandem.

We urge parliamentarians to pay close attention to this growing issue: 197 parliamentary constituencies are policed by the nine constabularies which have been identified to have purchased IMSI-catchers (the number of police forces with the technology is likely higher). The collateral collection of private data is, by its geographic nature, a constituency issue and should be treated as such.

Meanwhile, Police and Crime Commissioners (PCCs) have a professional obligation to respond to public concerns over policing matters, and therefore IMSI-catchers. According to the Association of Police and Crime Commissioners, the role of PCCs "is to be the voice of the people and hold the police to account."

Under the terms of the Police Reform and Social Responsibility Act 2011, PCCs must also set their force's budget. Police documents show that PCCs have, in their professional capacities, approved the acquisition of IMSI-catchers on behalf of their respective constabularies. If PCCs are to garner the confidence of the communities they purport to serve, then they must reconsider rubber-stamping IMSI-catcher acquisitions, and review this item with their constabularies as a matter of urgency.

[1] **The Bristol Cable online**, *Revealed: Bristol's police and mass mobile phone surveillance*, 10 October 2016.
[2] **The Ferret online**, *Prisoners outwit £1.2m mobile phone blocking technology*, 25 May 2016.

IMSI-Catchers & Civil Liberties

IMSI-catchers are indiscriminate surveillance tools that enable cell blocking, live tracking of mobile phone locations and identities, interception of text messages and phone calls, and even the distribution of malware, across a large radius.

Human rights groups in the UK strongly suspect that IMSI-catchers are in use by the State - but the purchase and deployment of these devices remain subject to inexplicable and unacceptable levels of secrecy.

Silkie Carlo
Senior Advocacy Officer
Liberty

However, an important Bristol Cable investigation in 2016 revealed that seven police forces were in possession of IMSI-catchers.[3] A 2017 VICE investigation[4] identified two further forces (Kent and Essex) to be in possession of IMSI-catchers.

The suspected use of IMSI-catchers for indiscriminate interception or hacking in the UK's public spaces[5] is highly likely to constitute a serious breach of fundamental human rights, such as the right to a private life, freedom of expression,

and freedom of assembly, as provided under the Human Rights Act 1998 (HRA).

We are concerned that, as with the onset of several unlawful surveillance practices, Parliament has not been consulted on the use of IMSI-catchers. Police forces will neither confirm nor deny their use of IMSI-catchers and consequently refuse to publish relevant statistical data or policies governing their use. Shielded by secrecy, the State's use of IMSI-catchers has been hidden from democratic accountability.

Liberty views the covert deployment of these military-style surveillance tools as a huge new challenge for civil liberties in the digital age.

The context of mass surveillance

The UK recently passed the Investigatory Powers Act – the most authoritarian surveillance legislation of any democracy in history.

The Act permits the retention of detailed communications data and internet records for the entire nation. It also permits mass interception and even mass hacking, as well as broad powers to hoard bulk datasets of personal information, interfering with the rights of many millions of people.

In addition to legal and policy questions, the use of IMSI-catchers raises a practical question: what do authorities gain from the deployment of IMSI-catchers that they cannot gain from other surveillance methods?

IMSI-catchers from some manufacturers permit the real-time interception and hacking of up to 1,500 handsets per minute across five networks within a potential range of 8km.[6] Thus, IMSI-catchers lend themselves to indiscriminate intrusion on whole groups of individuals within a location or at an event. Their highly secretive status risks their ever-increasing use with unchecked consequences. This deployment of covert, blanket surveillance in absence of prior suspicion is a chilling manifestation of the growing surveillance state.

Targeting locations and discriminating against communities

The indiscriminate intrusion on individuals within a large area cannot be considered necessary or proportionate, and does not constitute suspicion-led surveillance. In absence of any democratic accountability, we are deeply concerned about the locations that could be targeted.

[3] **The Bristol Cable online**, *Police remove documents following Cable Investigation*, 13 October 2016.
[4] **VICE online**, *More UK Police put cash down for IMSI-catchers*, 30 May 2017.
[5] **Sky News**, *Fake Mobile Phone Towers Operating in the UK*, 9 June 2015.
[6] **Document Cloud**, *202 Cellxion Product List*, uploaded on 28 October 2013.
[7] **VICE online**, *Phone Hackers: Britain's Secret Surveillance*, 14 January 2016.

An investigation for VICE[7] by technologist Dr Richard Tynan found evidence of the use of IMSI-catchers at London landmarks, where there is a very high footfall of people – innocent of any crime. One such landmark is the Palace of Westminster, which sees the frequent passage of tourists, democratically elected officials, constituents seeking confidential meetings, lawyers, civil society representatives working in pursuit of justice, journalists and lawful demonstrators.

"The use of IMSI-catchers at a protest or demonstration, for example, risks interference with the right to freedom of assembly as well as freedom of expression – rights that are fundamental to the health of British democracy."

Given the indiscriminate nature of IMSI-catchers, the disregard for multiple fundamental rights at the very heart of the UK's democracy is alarming.

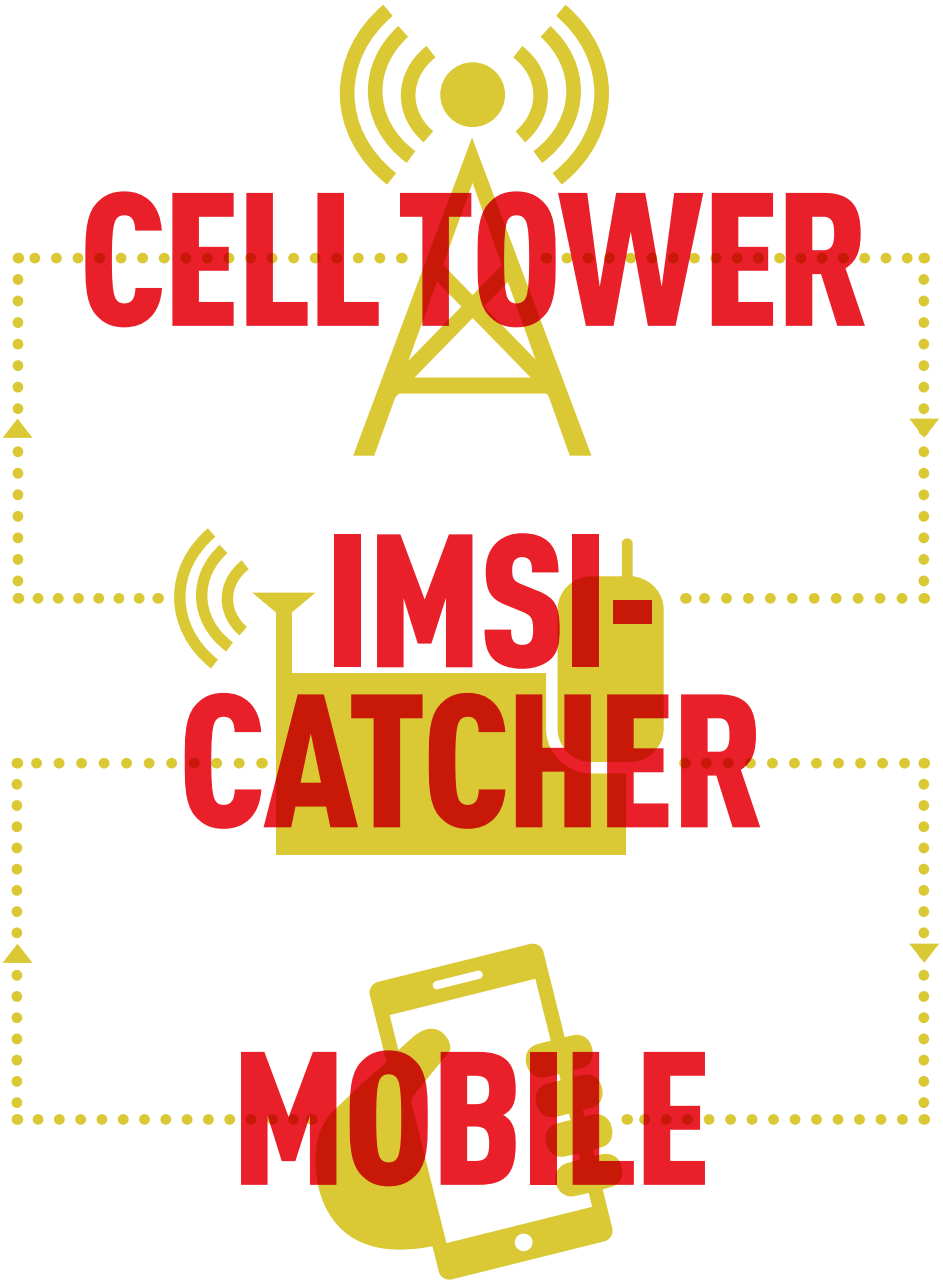
We are also very concerned that location-based IMSI-catchers may be used in a discriminatory manner that targets particular communities, institutions or places of worship. Such covert practices casting a shroud of suspicion over entire communities would be extremely damaging to affected groups and to wider community cohesion – not to mention a grievous breach of the prohibition of discrimination under the HRA.

Targeting events & freedom of assembly

We are very concerned that IMSI-catchers may be used to indiscriminately intrude on individuals in the vicinity of particular events – whether political protests, union meetings, community celebrations or informal gatherings. Targeting a lawful event for such intrusive covert spying would be a disturbing subversion of the principle of suspicion-led surveillance.

The use of IMSI-catchers at a protest or demonstration, for example, risks interference with the right to freedom of assembly as well as freedom of expression – rights that are fundamental to the health of British democracy.

Clearly, IMSI-catchers pose a grave risk to the health of civil liberties in the UK. We urgently require transparency of their use and a national conversation about the risks they pose, now.


CELL TOWER
IMSI-
CATCHER
MOBILE

IMSI-catchers, untargeted surveillance and the law

The legal basis for the roll-out of IMSI-catcher technology has always been unclear. *Neither confirm nor deny* ("NCND") policies mask public debate on the technology and obfuscate the powers which govern its use. Not until 2014 did a Minister suggest IMSI-catchers may be used on a combination of powers granted by the Police Act 1997; the Intelligence Services Act 1994 and in the Regulation of Investigatory Powers Act 2000 ("RIPA").[8]

Angela Patrick
Barrister
Doughty Street Chambers

Other sources suggest that the RIPA powers on directed covert surveillance – similar to long distance listening devices – were historically applied.[9] Little further explanation has ever been published.

The post-Snowden commitment to avow modern surveillance techniques in the Investigatory Powers Act 2016 ("IPA") has not brought any immediate clarity. The Act replaces the RIPA powers for interception, but leaves intact the RIPA powers on covert, directed surveillance and provisions of the Police Act 1997 and the

Intelligence Services Act 1994.[10] There are a range of powers in the IPA potentially broad enough to suggest an apparent legal basis the Government might seek to rely upon for IMSI-catcher use. That active and passive IMSI-catchers might perform a variety of functions and be used by a variety of agencies may explain a diversity of legal bases for their use; it cannot excuse legal uncertainty and a seemingly purposeful lack of transparency.

Equipment interference – or "hacking" – powers in the IPA are expected now to be used to cover the use of active IMSI-catchers by police and the intelligence agencies. So-called "targeted warrants" may cover interference with digital devices, including mobile phones, carried by multiple people or at one or more locations.[11] Thematic targeted warrants need very little in the way of recognisable targeting.[12] There is no requirement that any named individual or location be specifically linked to any reasonable suspicion that a crime has been committed. No named individual need be targeted nor does their connection to a specific crime need be specified.[13] There is arguably little to distinguish a thematic power of this breadth from a bulk general power.

Police warrants are granted in-house, subject to review by Judicial Commissioners.[14] This is not a form of judicial warrantry, but tests the proper decision making of police and others empowered to make surveillance warrants according to judicial review standards. This review can be delayed and authorisation delegated to junior officers, if "urgent".[15] Warrants must be "proportionate" and consider general privacy principles outlined in the Act (for example, whether its purpose might be achieved by less intrusive means).[16] The indiscriminate use of IMSI-catcher technology is unlikely to be proportionate and justifiable.

It is unclear how surveillance which fails to meet these standards might be challenged by individuals affected. Despite recommendations by civil society organisations, there is no provision in the Bill for general notification which would allow individuals to challenge any unlawful overreach in the use of broad and targeted warrantry. [17] In any event, NCND policies are routinely applied to deny the mere existence of IMSI-catchers.

The use of IPA powers by the police and agencies are limited to "serious" crimes. However these are broadly defined to include offences carrying a sentence of over three years imprisonment; or *any* violent crime *or* crimes done for unspecified "*substantial*" financial gain *or* where conduct is by a large

[8] **HL Deb, 11 Nov 2014, Vol 757, WA 24 (Lord Bates); see also HC Deb, 7 July 2015, WA 5369 (Mike Penning MP). For example, use of an active IMSI catcher could be considered property interference and potentially subject to s. 93, Police Act 1997. See Eric King and Matthew Rice,** *Behind the curve: When will the UK stop pretending IMSI catchers do not exist?*, Privacy International, 5 November 2017.

[9] **Guardian Online**, *Met police using surveillance system to monitor mobile phones*, 30 October 2011.

[10] **Authorities are expressly barred from using s.93 Police Act 1997 powers as an alternative to the IPA powers of equipment interference except in some limited cases of computer interference. See, for example, Section 14(1). However, for example, s.5 of the Intelligence Services Act 1994 remains in force.**

number of persons in pursuit of a common purpose.[18] So, not all kinds of crime must attract a significant punishment to trigger the use of the IPA. Since group conduct is covered, police and agencies might seek to rely on these powers for the investigation of public order offences arising from protest activities. Any investigation of violent crime or financial crime for "substantial gain" will open the door to the IPA. This threshold is less stringent than it might first appear, placing only limited restraint on State surveillance.

Intercept powers in the Act follow a similar model.[19] Compliance with the law is monitored by the new Investigatory Powers Commissioner ("IPCO").[20] IPCO replaces a range of previous oversight Commissioners – including the Surveillance Commissioner and the Interception of Communications Commissioner – whose effectiveness has been subject to historic criticism. Although the ICPO will now incorporate the Judicial Commissioners and will provide a final route of appeal for any official or agency refused permission to use surveillance; its function most visible to the public will be to provide after-the-event scrutiny. Codes of Practice which might better explain how these powers will be exercised remain a work in progress and the capacity of the IPCO remains untested. One early question must be whether and how will IPCO conduct effective public scrutiny in circumstances where the use of IMSI-catchers remains shrouded in secrecy.

The compatibility of untargeted surveillance – including IMSI-catchers - with the privacy rights in the Charter of Fundamental Rights for the EU ("the Charter") and the European Convention on Human Rights ("ECHR") remains subject to question. Untargeted surveillance is challenged by recent decisions of the Court of Justice of the EU ("CJEU") in *Watson & Ors v Secretary of State for the Home Department*[21] and by the Grand Chamber of the European Court of Human Rights in *Zakharov v Russia*.[22] In the first of these claims, the predecessor to the IPA 2016 was declared overbroad and unlawful. The IPA 2016 replicates much of the model criticised by the European Court of Human Rights. In the latter, the Russian framework for tapping of mobile phone data was insufficiently precise and lacked key safeguards. Both cases raise doubt over whether the safeguards introduced in the new Act are adequate and whether covert powers of surveillance can ever be used lawfully except when carefully targeted in connection with the most serious of criminal offences.

Domestic judges have been persuaded by the Government to ask the CJEU to think again.[23] The European Court of Human Rights is now considering a series of further challenges to UK law and untargeted surveillance.[24] The Government's insistence that the untargeted gathering of personal data poses little or no intrusion to individual privacy rights or to the public interest seems unsustainable and inconsistent with the approach at both European courts.[25]

Despite this continued uncertainty about the legality of the current framework in the IPA – and a real lack of clarity on the legal bases for the use of various forms of IMSI-catcher

– the roll-out of the technology appears to be gathering pace. Published contract data appears to reveal that at least nine UK police constabularies may be using IMSI-catchers now (see the first section of this briefing, above). As the devices become increasingly more capable, cheaper and more portable, the question of the legal basis for their use and the safeguards for our privacy can only become more pressing.[26]

Political hostility towards Europe means a legal answer from Strasbourg or Luxembourg is unlikely to be the last word on IMSI-catchers or other forms of untargeted and overbroad surveillance. Recalling Brexit, how the law protects our data remains key to future trading relationships (as *Schrems* illustrated for the US 'Safe Harbour' agreement.)[27] New legislation will bring the privacy guarantees in the EU General Data Protection Regulation into domestic law before May 2018. We are yet committed to the European Convention on Human Rights. We will remain a part of the Council of Europe, despite continuing tension on the role of the Court in Strasbourg. The crucial guarantees of the Human Rights Act 1998 continue to apply.

How the world views privacy, and what the rule of law means for its protection, remain critical issues as the UK seeks to assert its post-Brexit identity on a global stage. How and when we are willing to be observed by the State remain key questions not only for activists and constitutional scholars but for our future trading partners.

There is work for Parliament to do.

[11] **Section 101.**

[12] **Section 101**, *for example, makes clear that the warrant may cover a range of types of equipment and individuals or groups of individuals, or locations, not specifically related by reasonable suspicion to any particular crime.*

[13] **Ibid.**

[14] **Sections 106 – 110.**

[15] **Sections 106 – 107.** *Surveillance powers exercised under the Police Act and RIPA also involved in-house authorisation by police or agency forces, subject only to the oversight of the Surveillance Commissioner. The new IPA model introduces Judicial Commissioners whose powers are constrained to judicial review principles. The model does not adopt prior judicial authorisation, but instead adopts for judicial oversight of administrative decision making, albeit subject to significant exceptions for cases deemed urgent.*

[16] **Section 2(2)(a).**

[17] *The circumstances when the Act provides for notification are very limited. Section 231 provides for error reporting by IPCO in respect of any "relevant error" relating to that person of which the Commissioner is aware if the Commissioner considers that (a)the error is a serious error, and (b)it is in the public interest for the person to be informed of the error. The IPCO may not decide that an error is a serious error unless the Commissioner considers that the error has caused significant prejudice or harm to the person concerned. Simply because an error causes a violation of Convention rights does not render it serious.*

[18] **Section 263.**

[19] **Sections 15 – 43.** *Warrants may be granted by the Secretary of State on grounds of serious crime, national security or harm to the economic interests of the UK, subject to review by the Judicial Commissioners. These powers might be applied in cases of passive IMSI-catcher use, focused on the interception of information being communicated by devices.*

[20] **Sections 227 – 240.**

[21] **Watson v Secretary of State for the Home Department**, *Cases C-203/15 and C-698/15.*

[22] **Roman Zakharov v Russia (Application no. 47143/06)**, 4 December 2015, *para 250.* See also **Szabó and Vissy v. Hungary (Application no. 37138/14)**, 12 January 2016, *para 73* and **Bykov v Russia App No 4378/02**.

[23] **Privacy International v the Secretary of State for Foreign and Commonwealth Affairs and Others**, *UKIPTrib IPT_15_110_CH*, 8 September 2017.

[24] See, for example, **Big Brother Watch and others v UK**, *App No 58170/13;* **10 Human Rights Organisations v UK**, *App No 24960/15.*

[25] **S & Marper v United Kingdom**, (2009) *48 EHRR 50.*

[26] **Naarttijärvi, M.**, *Swedish police implementation of IMSI-catchers in a European law perspective, Computer Law & Security Review (2016), p37.* Available at http://dx.doi.org/10.1016/j.clsr.2016.07.006

[27] **Case C-362/14.**

The Bristol Cable recommendations

To date, 197 Parliamentary constituencies are known to be policed by constabularies with IMSI-catchers. The number of constabularies with the surveillance technology is most likely far higher. The time has come for UK public authorities to uphold their commitment to transparency and policing by consent by disclosing information on IMSI-catchers, and to come clean on 'law enforcements' worst kept secret'.

Unfortunately, to date the Home Office and police have been less than forthcoming on this matter. This briefing recommends that Members of Parliament urgently investigate IMSI-catchers on behalf of their constituents. Scrutiny on the use of such technology would provide an important first test of the Government's approach to surveillance powers and privacy following the adoption of the IPA 2016.

A short, focused Select Committee inquiry could provide a vital and important opportunity for cross-party post-legislative scrutiny, incorporating a thorough Parliamentary assessment of the unique range of rights and civil liberties impacts presented by this particular form of emerging and intrusive technology.

This briefing recommends MPs and Peers pursue the disclosure of the following information to facilitate any Parliamentary enquiry and to inform the effective public scrutiny of IMSI-catcher technology by the IPCO:

1. All Home Office and police governing guidance pertaining to IMSI-catcher authorisation and deployment.
2. All Home Office and police governing guidance pertaining to the treatment and retention of data obtained via IMSI-catchers.
3. A historical statistical overview, to date, of IMSI-catcher deployment by all public authorities, including respective anonymised operational details.
4. Public authority owned or operated IMSI-catcher model type/s, value and date of all respective contracts, and company names of contractor/s and supplier/s.

Which constabularies own and operate IMSI-catchers?

Although the number is likely higher, nine UK constabularies have purchased IMSI-catchers according to Bristol Cable research. These constabularies serve 197 parliamentary constituencies.

Bristol Cable research has revealed that the acronym, 'CCDC', stands for Covert Communications Data Capture, and has been used by police forces nationally. The acronym has operated to classify the purchase of IMSI-catchers.

The constabularies identified:

1. **Avon and Somerset**
2. **West Midlands**
3. **Warwickshire**
4. **Metropolitan**
5. **South Yorkshire**
6. **Kent**
7. **Essex**
8. **Staffordshire**
9. **West Mercia**

Metropolitan Police:	The Metropolitan Police paid Cellxion, a firm that manufactures IMSI-catchers, £1m for 'CCDC equipment' in 2015.
Avon and Somerset Constabulary:	Avon and Somerset constabulary paid Cellxion, a firm that manufactures IMSI-catchers, £169,575.00 for 'CCDC equipment' in 2015-16.
West Midlands Constabulary:	West Midlands constabulary contracted with Cellxion in 2015, a firm that manufactures IMSI-catchers. Unredacted police meeting minutes from 2016 state: "West Midlands and Staffordshire Police have recently purchased and operated 4G-compatible CCDC equipment."
Warwickshire Constabulary:	Unredacted police meeting minutes from 2016 record that the Police and Crime Commissioner for Warwickshire approved a decision to replace their force's existing equipment and purchase new CCDC technology in 2017/18.
West Mercia Constabulary:	Unredacted police meeting minutes from 2016 record that the Police and Crime Commissioner for West Mercia approved a decision to replace their force's existing equipment and purchase new CCDC technology in 2017/18.
South Yorkshire Constabulary:	A South Yorkshire Constabulary 2015/16 budget item called "IMSI Covert Communications" was earmarked £144,000. A separate line in the same budget – again called "CCDC" – was allocated an identical amount: £144,000. South Yorkshire constabulary confirmed that 'CCDC' and 'IMSI Covert Communications' were the same budget item.
Kent Constabulary:	Essex Constabulary allocated a total of £145,000 to "CCDC Platform Equipment", according to a budget spreadsheet for spending between 2016 and 2019. The budget marks the CCDC expenditure as "joint with Kent. Kent Constabulary had published a document – which was later removed – which also listed its CCDC capacity.
Essex Constabulary:	Essex Constabulary allocated a total of £145,000 to "CCDC Platform Equipment", according to a budget spreadsheet for spending between 2016 and 2019.
Staffordshire Constabulary:	Unredacted police meeting minutes from West Mercia and Warwickshire Constabularies in 2016 state: "West Midlands and Staffordshire Police have recently purchased and operated 4G-compatible CCDC equipment."