Home Office

A Post-Implementation Review Report

The Telecommunications Restriction Orders (Custodial Institutions) (England and Wales) Regulations 2016.

2016 No. 830

August 2021

This publication is available at www.gov.uk/government/publications and www.legislation.gov.uk.

Any enquiries regarding this publication should be sent to us at SOCPolicingUnit@homeoffice.gov.uk.

Contents

Aim of report

- This report has been prepared by the Home Office to assess whether the Regulations governing Telecommunications Restriction Orders (TROs) have met the intended objectives of the legislation. A post-implementation review was mandated as part of this secondary legislation within five years of their coming into force in 2016.

- The Regulations stipulated that the Secretary of State must:

    - Carry out a review of these Regulations, and publish a report setting out the conclusions of the review.
    - The report must in particular—
        - Set out the objectives intended to be achieved by these Regulations,
        - Assess the extent to which those objectives are achieved,
        - Assess whether those objectives remain appropriate, and
        - If so, assess the extent to which they could be achieved in another way which involves less onerous regulatory provision (within the meaning given by section 32(4) of the Small Business, Enterprise and Employment Act 2015(1)).
        - The first report must be published no later than five years after these Regulations come into force.
        - Subsequent reports must be published at intervals not exceeding five years.

- This review is underpinned by case studies of the two occasions TROs have been used operationally with an additional example of when a TRO was planned for but not ultimately used. This has enabled an assessment of the operational benefits these Regulations have delivered and the economic implications of using such orders. This has informed the assessment of the extent to which their objectives have been met.

Objective

- A Telecommunications Restriction Order, as set out in the legislation, is:

    - ‘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.’

- The objective underpinning these Regulations is to reduce crime by tackling the illegal[1] use of mobile phones by prisoners in a custodial institution. This provides a unique capability, enabling law enforcement to apply for a court order to compel Mobile Network Operators (MNOs) to remotely deactivate multiple mobile phones in prisons. Without a TRO, MNOs would not be obliged to act on a request from law enforcement to deactivate an unauthorised mobile phone in the possession of a prisoner.

- TROs allow law enforcement and HM Prison and Probation Service (HMPPS) to cut off a prisoner’s capacity to communicate with individuals in and outside of prison without authorisation or supervision from HMPPS. This includes serious and organised crime (SOC) and individuals charged with terrorism and extremism offences. This affords law enforcement and HMPPS the opportunity to fully deactivate devices in a timely manner, thereby stopping or mitigating the impact of crime that mobile phones enable.

- Prisoners have a number of lawful and authorised avenues to communicate with individuals outside of prison such as through the PIN phone system. This is a secure phone service used by prisoners to call approved contacts which can be supervised by HMPPS. Therefore, prisoners do not have the necessity nor the authorisation to carry and use mobile phones. When prisoners possess and use unauthorised communication devices, such as mobile phones, this is both illegal and it is likely that they are engaged in crime. That can impact prisons and communities, as mobile phones enable prisoners to continue to commit crime beyond the prison walls.

[1] As stipulated under section 40D (3A) of the Prison Act 1952.

Background

- The use of unauthorised mobile phones and SIM cards in prisons in England and Wales is a significant and escalating problem. Their use threatens good order and discipline across the entire custodial estate as a key enabler of crime, SOC and terrorism. The clearest picture we have is provided by the HMPPS Annual Digest 2019/20[2] which highlighted that in the 12 months up to March 2020 there were almost 12,000 incidents where mobile phones were found, and approximately 5,500 incidents where SIM cards were found in prisons. This equates to roughly 30 or more mobile phones found per day across the custodial estate. HMPPS Digests since 2017 also makes clear that the confiscation of illicit mobile phones and SIMs has steadily increased year-on-year.[3]

- HMPPS assess that mobile phones are key enablers of SOC, widely used to allow such offenders to continue local and national criminality almost unhindered. HMPPS also assess that mobile phones are a key component in organising and facilitating the smuggling of contraband into prisons. This fundamentally undermines the prison wall, allowing SOC offenders to continue running their criminal businesses in communities, from county lines and drug supplies blighting our streets, to organising serious violence and murders from prison cells.

- The threat mobile phones represent to safety in prisons and communities extends to individuals imprisoned under the Terrorism Act 2000. HMPPS report that prisoners convicted of extremism and terrorism offences have been found in possession of or to have access to mobile phones and through such devices the internet. This provides an avenue for these prisoners to continue to offend while in custody.

- Rapid technological change has enhanced the ability of prisoners to smuggle mobile phones into prisons. Devices continue to be miniaturised while becoming ever more technically capable. This has driven a decrease in the relative cost of mobile phones in prisons reflecting their increasing availability.

- The Government has taken measures to address this significant and ever-changing threat. This included legislating for the TRO, to provide law enforcement with the power to apply to the court for an order to compel MNOs to remotely disconnect unauthorised mobile phones in use and inside prisons. This negates the need for HMPPS to first take physical possession of the device to deactivate it.

- The Home Office introduced enabling legislation in the Serious Crime Act 2015 (SCA 2015) providing this regulation-making power that would allow law enforcement to apply to the courts for a TRO. This order requires a communications provider to take

[2] HMPPS, *Annual Digest 2019/20*, (30 July 2020 and updated on 10 June 2021)

[3] HMPPS, *Annual Digests 2017/18 – 2019/20*

whatever action the order specifies for the purpose of preventing or restricting the use of communication devices by persons detained in custodial institutions. Disconnecting and/or blacklisting unauthorised mobile phones puts those devices beyond normal operational use. This filled a legal and operational gap as up until 2016 MNOs were not legally obliged to disconnect devices contributing to crime from within custodial institutions even if requested to do so by law enforcement. The legal framework for TROs set out in the Regulations came into effect in August 2016.

- This power delivers a unique capability to law enforcement and HMPPS. It enables for the mass disconnection of all mobile phones identified as unauthorised in an establishment. Without the ability to compel MNOs to remotely deactivate a mobile phone, law enforcement and HMPPS would have to rely upon MNOs agreeing to voluntarily disconnect unauthorised mobile phones in prisons.

- The courts grant a TRO when they are satisfied 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. A TRO must specify a date on or before which the requirements of the order are to be complied with and an application can only be made on behalf of the Secretary of State, Director General of the National Crime Agency, HMRC commissioners, or a chief officer of police. TRO hearings are heard by a District Judge in a County Court[4], in private, who considers the application, its terms, supporting evidence including the required witness statements.

- TRO legislation complements the Prisons (Interference with Wireless Telegraphy) Act 2012 and the Investigatory Powers Act 2016. These two Acts provide law enforcement and HMPPS with the legal means to source and identify illicit communication devices in prisons. The TRO provides the disruption element, enabling law enforcement and HMPPS to request MNOs to remotely deactivate the unauthorised mobile phones that have been found.

- The alternative tactical options available to law enforcement and HMPPS to deploying a TRO include:

    - Delivering a specific prison wing or prison wide search. Doing so cannot guarantee all mobile phones are found as once a search begins prisoners can hide or dispose of illicit items. Conducting a search on this scale is also a costly, resource intensive and complex undertaking that can be disruptive to the good order and discipline in an establishment.

    - Installing permanent phone signal blocking technology. This a costly and complex capability to deploy in an establishment, necessitating ongoing costs to run and maintain this technology.

[4] The court that hears TRO applications at this time is Clerkenwell and Shoreditch County Court.

Summary of case studies

- TROs have been available to law enforcement and criminal justice partners since 2016 and have been used twice operationally.

- They have been used to target sex offenders, drug dealers and violence impacting good order, discipline and safety in prisons as well as the ability of criminals to penetrate the prison wall and continue to harm communities.

- The following three case studies include those two operational examples and the only other time agencies had planned to apply for a TRO. These examples have been summarised to explain when they occurred, which agencies participated, and what the operational outcomes were. These findings have informed an assessment of the operational benefits these Regulations can deliver in the section that follows.

Operational Case Studies
Case study 1
Location: London
Date: 2017
Primary agency included: HMPPS
Category: B[5]
Summary: The first use of a TRO was a successful proof of concept that the TRO application process could be successfully navigated, that all MNOs were willing to collaborate in the TRO process, and deployment could derive impactful outcomes. In addition, the TRO deployment was contained, with no members of the general public submitting complaints suggesting no phone services were affected outside the prison boundaries.

[5] Represents a closed male prison, for offenders whose assessed risks require that they are held in the closed estate and who need security measures additional to those in a standard closed prison.

Operational Case Studies
Case study 1
Impact: Seizures included: mobile phones, drugs, a knife and bank details Total number of mobile phone numbers disabled: 160 authorised to be disabled, with 88 actually disabled. The number of mobile phones and SIMs disconnected were less than intended due to the time it took to navigate the application process and secure the order, which included preparing the intelligence package and TRO application to the court, and the hearing process that considered the application. Therefore, the disconnections were seen as a fraction of the overall number of mobile phones in circulation.
Learning: That TROs work, the application process can be navigated, and MNOs are willing to collaborate to support TRO deployments. The time taken to evidence the devices that needed to be disconnected, and the steps required to seek a TRO took longer than expected and required more staff resources than envisaged.
Case study 2
Location: East England
Date: 2019
Primary agency included: HMPPS
Category: C[6]

[6] Represents a closed male prison, for offenders who are assessed as requiring standard closed conditions, and do not need additional security.

Operational Case Studies
Case study 2
Summary: This operation was designed to identify and disrupt the illicit use of mobile phones in this prison. A TRO was viewed as potentially part of tactical plans as the means to deactivate the identified phones and therefore help disrupt offending if it was found. However, a TRO was not sought as suitable devices were not located within the prison which reached the necessary thresholds to request action by an MNO during this time bound operation. The threshold relates to how confident HMPPS were that devices were present in the prison. A further TRO deployment was not pursued as it was not deemed operationally viable at that time.
Learning: A TRO deployment remained a viable option and should remain part of tactical planning and collaboration between law enforcement and HMPPS, but only used when tactically required. This TRO tactical development and planning also strengthened collaboration between partners that contributed to future TROs being considered and deployed.
Case study 3
Location: North West England.
Date: 2021
Primary partners included: Police and HMPPS
Category: B

Operational Case Studies
Case study 3
Summary: The use of a TRO in this case was part of a wider multi-agency operation to disrupt the supply of illegal items into the prison including mobile phones. In this case the police were the applicant for the TRO supported by HMPPS.
Impact: Seizures included: mobile phones, SIMs and drugs Total number of handsets/devices disabled: 229 Total number of SIMs disconnected: 247 More widely there were a number of arrests made both in the prison and the community as part of the wider operation. Prosecutions are being progressed in these cases. Thousands of texts were sent to numbers contacted by those disconnected phones, warning that it is an offence to contact an unauthorised mobile phone in prison.
Learning: A joint approach to disrupting unauthorised mobile phones and SIMs in prisons is required to effectively bear down on their use and the crime and harm they enable. With each agency playing to their strengths and collaborating with MNOs to disconnect mobile phones as part of a larger and integrated tactical plan.

Economic assessment

- Due to the lack of evidence and data around the outcomes and benefits around TROs, it has not been possible to conduct a full economic assessment.

- TROs have been deployed twice and disconnected a total of 317 devices during these deployments. Some of these devices will have been used for criminal activities, both SOC and non-SOC. However, the proportion used for criminal activities or SOC activities is unknown.

- There is potential for a TRO to be good value for money (VfM) due to the high harm and high value nature of SOC, which has a cost to society of £37 billion per year, but the small sample of deployments and lack of data does not enable a robust assessment.

Available evidence and data

- TROs have been deployed twice, which is less than anticipated. The reasons for this are outlined in the following consultation findings section.

- A total of 317 phones were deactivated. However, it is not known how many of these were used for SOC related purposes.

Costs:

The total cost of deploying a TRO is estimated to be between about £2,000 and £20,000 with a considerable degree of uncertainty. This is based on the updated costs to HMPPS, HMCTS, the police and MNOs. The difference between the lower and upper bound is the number of disconnections applied for in the TRO.

A breakdown of some of the costs is provided below. A full breakdown of the overall costs and ranges have not been disclosed because of the sensitive nature of these operations but have been included in the overall estimate.

- The standard court fee for considering a TRO application = £353.
- Average HMPPS cost for intelligence work to inform a TRO = £1,250 to £5,000.
- Average police cost to apply for and support a TRO = £1,000 to £3,000.[7]
- Average costs to MNOs to action TRO related requests = £500.[8]

[7] In the two cases where a TRO was deployed, there were no additional police costs as they were absorbed into existing operational budgets.

[8] Based on an estimated cost of £250 per day, and an average of two days required per TRO.

Using the case studies sighted, the expected and actual costs, benefits and implications of deploying a TRO have been compared in the following table.

Expected vs actual outcomes	
Expected	**Actual**
The overall cost to HMPPS and HMCTS for considering and deploying 4-16 applications per year was estimated at costing £3.3 million over 10 years.	This cost was not borne out in reality as there were only two TRO deployments over the five-year period since the legislation came into force.
Cost breakdowns: Cost to HMPPS: • Legal costs of around £5,200 in year 1, £10,500 in year 2, £20,500 in years 3 and 4 (£1,300 per TRO application). • Procurement costs of £200,000 in year 1, 2 and 3. • Staffing costs of around £27,500 in year 1, £60,000 in year 2, £59,500 in years 3 and 4. • Evidence analysis costs of £27,500 in year 1, £55,100 in year 2, £109,000 in years 3 and 4. • Annual costs of approximately £200,000 in years 4 to 10. Average annual cost: £45,000 incurred by HMCTS.[9] **Alternative option:** HMPPS cost, signal blocking equipment: • £300 million to fit mobile phone signal blocking equipment across the estate. • £0.8 million per year in maintenance costs.	There has been no ongoing cost due to HMPPS not establishing a full time TRO team as envisaged. Total costs incurred by HMPPS and police for securing two TROs were absorbed into existing operational budgets.[10] An average cost for a TRO can be between £2,000 to £20,000 depending on the operational approach taken. This estimate is variable as it depends on the operational aims, investigatory techniques used and tactics employed. The vast majority of costs are incurred by the applicant, with some cost to MNOs as detailed below.

[9] The HM Courts and Tribunals Service charge a standard Court Charge of £353 for processing a TRO, contributing to covering some of these costs.

[10] Each example approached deploying a TRO differently, therefore, further operational examples are needed to inform an accurate average deployment cost.

Expected vs actual outcomes	
Expected	**Actual**
Annual cost: £30,000 to £120,000 incurred by MNOs.[11]	In the original IA, MNOs were expected to incur costs for legal representation of £950 per court order and additional staffing of £3,800 per court order. These costs did not materialise based on the two case studies as no legal representation was required. However, MNO's may need up to two days of work to action a TRO, or a cost to the application in the region of £500.[12]
Savings to society deemed too difficult to predict against.	There is insufficient evidence to quantify savings to society at this time. There was a total of 317 mobile phones and 247 SIMs deactivated due to these two operational examples and there is an expectation that this may have resulted in disrupting crime enabled by the unauthorised use of these mobile phones.
The Regulations would have no net impact on business.	There has been no net impact on business as MNOs have been reimbursed when required and court fees paid by the applicant.
There would be no increase in wage costs.	There has not been an increase in wage costs, as the bespoke TRO team in HMPPS has not been established, and resource costs associated with the two TRO operational examples were absorbed into existing police/HMPPS budgets. In future a resource cost may be incurred.
There would be 4-16 County Court applications per year.	There have been two applications in five years.

[11] In the TRO legislation there is provision for the court to stipulate as part of the order that the applicant pays any or all of the costs likely to be incurred by a communications provider.

[12] Staffing costs that were charged by an MNO were fixed at £250 per day.

Expected vs actual outcomes	
Expected	**Actual**
The approach to tackling unauthorised mobile phones focused on disconnecting these devices.	The approach has been refined focusing on the intelligence dividend and attributing a crime before disconnection when tactically required.
The deployment of capabilities under a TRO were viewed in isolation.	The deployment of capabilities under a TRO are now viewed as part of an integrated tactical approach. Focusing on intelligence led surveillance of targeted individuals and attribution of those devices and the crimes they enable to individual offenders, ahead of actioning a TRO.
Completing a TRO application would take 27 days.	Completing a TRO application has taken roughly 4-6 weeks, with the Court process navigated in between 10 to 21 working days

Consultation findings

This review is underpinned by a consultation conducted by Home Office officials with Government officials, all four MNOs, and law enforcement and criminal justice partners connected to the adoption of these Regulations and their operational use. The consultation included colleagues from the Home Office, police (including Greater Manchester Police, the North West Regional Organised Crime Unit and the National Prison Intelligence Coordination Centre), Ministry of Justice, the Civil Procedure Rules Committee, HMPPS (including the Security, Order and Counter Terrorism Directorate, and HMP Forest Bank), all MNOs (BT, O2, Three and Vodaphone), and HMCTS (namely the Clerkenwell and Shoreditch County Court).

Through this consultation and the aforementioned case studies the following findings were evidenced. These findings are split into three overarching areas:

- To understand the original operational approach and why that has not been fully delivered.
- The new approach HMPPS and law enforcement are taking to effectively target the unauthorised use of mobile phones in prisons.
- How TROs can be effective in the future.

These findings were ultimately derived from two operational case studies. Additional operational examples are required to properly evidence whether the objectives of the TRO legislation have been met. As well as to strengthen our understanding of the impact and value TROs can deliver in supporting law enforcement and criminal justice partners to target the illicit use of communication devices and the crime and harm they enable in prisons and into communities.

Original operational approach

- On adoption the intention had been to use TROs to regularly disconnect illicit mobile phones in prisons. To deliver this blanket approach there had been an ambition to establish an HMPPS team to manage TRO applications. That would be supported by the acquisition of equipment to disconnect communication devices in prisons by both HMPPS and the police.

- This approach was expected to be cost-effective and impactful, with no net financial impact on business (that is, the MNOs). The intention was to meet this escalating threat head on by blacklisting as many mobile phones and SIMs illicitly used in prisons as possible. Since the Regulations came into force MNOs have been broadly supportive of using it, for retaining the Regulations and have not requested the Regulations are revoked.

- However, the dedicated TRO team in HMPPS was not established once it became clear to HMPPS operational staff that the time and resources required to identify unauthorised communication devices, collect and deconflict identified phone numbers, and then navigate the court process was greater than originally envisaged.[13] As an example, the court process can take anywhere between 10 to 21 working days to navigate. This is an inhabiting factor to applicants for the ability to move at pace to identify, attribute (if tactically deemed necessary) and disconnect mobile phones is critical to successfully disrupt the criminality mobile phones enable, and to secure such devices through targeted searches before they can be disposed of.

- There has also been a system-wide lack of understanding on what a TRO is, how to apply for it and the outcomes that can be delivered through an order. This has inhibited the number of applications made by law enforcement and HMPPS.

New approach to the threat

- The approach HMPPS now take to address the threats emanating from the unauthorised use of communication devices in prisons requires a change in how TROs are approached and viewed. This approach centres on intelligence gathering and attribution. The dividends from understanding and attributing a crime to an offender in prison can outweigh the benefits from focusing only on disconnecting a mobile phone or SIM without identifying the user.

- This new approach was driven and enabled by the significant investments the Government has made in HMPPS capacity and capability[14], particularly in intelligence gathering and assessment. HMPPS now has far more nuanced resources at its disposal than it did in 2016 to address the illicit use of communication devices, and SOC in the round.

- This new approach also aims to cut off the conveyance of illicit communication devices into prisons, as the devices in use in a prison are targeted and disrupted. This necessitates collaboration between law enforcement and HMPPS, with police now preferring to use HMPPS capabilities and resources to disrupt phones inside a prison[15] as police focus on cutting off the flow of contraband into establishments.

---

[13] The difference between expected and actual time requirements is highlighted in the ‘expected vs actual outcomes’ table in the economic assessment section.

[14] This has included establishing the Police managed Regional Prison Intelligence Units, and the HMPPS managed Serious and Organised Crime Unit, the Sensitive Intelligence Unit, and the National Intelligence Unit, among other initiatives including the acquisition of a range of capabilities designed to block and disconnect unauthorised communication devices in prisons.

[15] Such collaboration impacts the illicit economy by creating an increased demand for mobile phones following a successful TRO deployment. A barometer of a successful operation, the consequences of which HMPPS work to mitigate.

- TRO deployments support this new approach as the Regulations represent the disruption element to the intelligence gathering powers law enforcement and HMPPS have in the prison environment.

How to deliver TROs effectively

- TROs can no longer be viewed as a tactic to be used in isolation. Instead, TRO's must complement other tactical options available to law enforcement and HMPPS and only to be used when tactically necessary. As an example, law enforcement and HMPPS may desire to focus on intelligence dividends from a communication device, rather than seeking to deactivate that device in the first instance.

- A multi-agency approach is required to make TROs fully effective. With police and HMPPS in particular working in tandem, utilising their strengths to deliver an impactful outcome.

    - Police apply for the TRO and navigate the court process to secure the TRO. HMPPS deploy their capabilities to gather the intelligence to identify, attribute (if tactically deemed necessary) and then disconnect multiple mobile phones and SIMs with MNO collaboration.

    - TRO deployment should be complemented by a joint police-HMPPS effort to deter the smuggling of contraband into a prison and stem the flow of illicit mobile phones and SIMs entering the custodial estate. This should be followed by efforts to address the consequences of successful operations as offenders will seek new avenues to convey illicit articles into prisons, once demand for communication devices increases.

    - This approach can significantly reduce the availability of unauthorised communication devices and disrupt the crime these devices enable.[16]

- To make gains sustainable TROs should be applied effectively and persistently over the longer term, to relentlessly degrade both the use and availability of illicit mobile phones and SIMs. Multiple deployments in a prison over a number of months would make criminal communications more difficult and riskier to undertake and therefore disrupt prison-generated crime far more thoroughly.

- Given the progress HMPPS and police have made to address the unauthorised use of mobile phones, SIMs and SOC in prisons, a reduction in mobile phones in circulation should make a TRO more effective in the future. The field of potential targets would be narrowed, enabling more impactful analysis and improving the chances of attribution and therefore criminal justice outcomes.

[16] The 3rd case study provides an excellent example of what a multi-agency response and joint tactical approach can deliver through a TRO.

- The application process could be streamlined, by exploring whether a court could grant applications outside of a formal hearing, to reduce the time required to secure a TRO.
- Further, the application process could also be made more accessible by expanding the number of courts eligible to grant a TRO application. Only the Clerkenwell and Shoreditch County Court can hear applications at this time.
- The only financial costs associated with TROs are when they are applied for and deployed. Costs could be further reduced if police continue to collaborate with HMPPS, utilising each other's skills and capabilities. With police deploying their resources outside of a prison to stem the flow of contraband through the prison wall, and HMPPS deploying their resources to gather intelligence and disrupt unauthorised mobile phones within a prison.
- All of these efforts could be strengthened by delivering an effective communication campaign with law enforcement and criminal justice partners to improve system awareness of the TRO and what it can deliver.

Conclusion

This report aimed to assess the extent to which the objectives underpinning the TRO have been achieved, and the extent to which those objectives remain appropriate. Notwithstanding the position that a full economic assessment of the TRO cannot be performed at this time, the following reflections and conclusions were informed by this consultation and from the operational learning law enforcement and criminal justice partners have derived from the aforementioned case studies.

- The number of seized mobile phones is significant and growing, therefore the threat posed by illicit communications is escalating. In the 12 months up to March 2021 almost 12,000 mobile phones were seized[17] or roughly 30 or more mobile phones were seized per day from across the custodial estate. This is compared to 11,500 incidents in the previous 12 months to March 2019[18] and 10,600 incidents in the year to March 2018.[19]

- The alternatives to using a TRO can be more costly, timing consuming and complex to deliver, such as conducting regular prison searches or deploying expensive equipment to permanently block phone signals across an establishment.

- The crimes that these two TRO operational examples disrupted include drug dealing, the smuggling of drugs and contraband into a prison and money laundering among other SOC related crimes.

- The TRO can also be impactful when used, as it can permanently deactivate hundreds of mobile phones in a particular prison on a single day. This can be achieved without the need to first take physical possession of a communication device.

- The TRO also has no net financial impact on business (as assessed in the TRO Validation Impact Assessment compiled ahead of these Regulations coming into force) as MNOs can be reimbursed for the costs incurred complying with an order.

- Additional operational examples are also required to deliver a strengthened evidence base to enable a more robust monetised assessment of these Regulations to be made. While time is required to deliver outcomes that can be modelled from the two available case studies. For instance, the arrests derived from the second TRO deployment will take time to translate into potential criminal convictions.

[17] HMPPS, *Annual Digest 2019/20*, (30 July 2020 and updated on 10 June 2021)

[18] HMPPS, *Annual Digest 2018/19*, (25 July 2019 and updated on 19 March 2020)

[19] HMPPS, *Annual Digest 2017/18*, (26 July 2018)

TRO objectives

- The strategic objective is to reduce crime. The TRO is a court order that compels MNOs to disconnect identified unauthorised mobile phones in a prison. To disrupt the illegal use of mobile phones by prisoners and provide law enforcement and HMPPS with a capability they do not otherwise have, to remotely deactivate multiple mobile phones that enable prisoners to continue to offend.

Extent these objectives have been met

- The two operational case studies demonstrate what a TRO can deliver in disrupting the unauthorised use of mobile phones in prisons. The aims of these two examples, to identify, attribute and disconnect a large number of unauthorised mobile phones in those two establishments, were broadly met. However, the extent to which they disrupted criminal activity was unable to be assessed due to a lack of evidence and data around the two deployments, and therefore it is unknown to what extent the objectives underpinning the rationale for TROs have been achieved.

Extent these objectives remain appropriate

- The significant and escalating threat represented by the unauthorised possession and use of mobile phones requires a robust response by Government, law enforcement and HMPPS. The TRO allows for the remote disconnection of multiple mobile phones removing the need to first take physical possession of the device. This is important as it can be operationally difficult to physically find the device and to do so before prisoners can use that device to commit crime.

- Prior to the adoption of the TRO, law enforcement and HMPPS relied upon the goodwill of MNOs to voluntarily cooperate with law enforcement requests for unauthorised mobile phones to be deactivated in prisons. TROs provide both the means to compel MNOs to deactivate unauthorised mobile phones in prisons, and provide MNOs with the legal cover to action such requests.

- The alternative tactical options available to the TRO include regular prison searches to seize illicit communication devices, or deploying technology to block phone signals across an establishment. These options can be more operationally resource intensive, complex and costly to deliver.

- Therefore, the objectives of the TRO remain appropriate, as it provides a unique tactic against a growing threat to good order and discipline in prisons and safety in communities. It can also be a cost-effective tactic when compared to alternative tactical options.

- Revoking these Regulations will also not deliver any benefits or net cost savings to government or business.

Extent these objectives can be achieved another way

- No other measure provides the legal means to compel MNOs to remotely deactivate multiple mobile phones. This remote deactivation cannot be achieved without MNO collaboration.

- Prior to the adoption of the TRO, law enforcement and HMPPS relied upon MNO's voluntarily supporting efforts to disrupt the illegal use of mobile phones by prisoners. The TRO made it a legal requirement for MNOs to deactivate mobile phones in prisons if compelled to by a court order, which in turn provided MNOs with the legal cover to action those deactivations, and an agreed process to reactivate incorrectly deactivated mobile phones (such as mobile phones that were not part of the order or were outside of the custodial establishment).

- This means that the objectives of the TRO could only be achieved outside of this legislation if MNOs voluntarily agreed to deactivate unauthorised mobiles phones in a prison. However, all parties, including MNOs, prefer actioning deactivations if mandated to do so by a court order.

Recommendation

It is the recommendation of this report that the TRO is retained, and these Regulations are promoted.

- This Reviews consultation made clear that the threat from the unauthorised use of mobile phones in prisons is significant and escalating. That the TRO fills an operational gap, providing a unique tactic, which can be a cost-effective when compared to alternative tactical options, and when deployed, a TRO has been impactful.

- However, as there have been two operational examples since its adoption in 2016, there is not sufficient evidence to inform a robust assessment of the extent to which the objectives of the TRO have been met.

- The consultation provided clear reasons why TROs have not been used as often as anticipated. For example, a lack of awareness among law enforcement and HMPPS, the approach HMPPS take to address this threat has changed, and the process for securing a TRO was more complicated and time consuming than expected.

- Promoting the use of the TRO would gather additional operational examples and thereby provide an evidence base to make a more informed decision in a future Review as mandated in these Regulations.