



Prisons and Interference with Wireless Telegraphy

Consultation Document

Channel Islands Competition and Regulatory Authorities

Document No: CICRA 13/07

February 2013

*Guernsey Competition and Regulatory Authority
Suites B1 & B2, Hirzel Court,
St Peter Port, Guernsey, GY1 2NH
Tel: +44 (0)1481 711120
Web: www.cicra.gg*

*Jersey Competition Regulatory Authority
2nd Floor Salisbury House, 1-9 Union Street,
St Helier, Jersey, JE2 3RF
Tel: +44 (0)1534 514990
Web: www.cicra.je*

CONTENTS

1. Introduction.....	2
2. Purpose and Structure of the Consultation	3
3. Legislative Background	4
4. Background to the development of legislation	5
5. Areas for comment	7
Annex	8

1. Introduction

The presence of wireless telegraphy devices, in particular, illicit mobile telephones presents serious risks to the security of prisons and other similar institutions, as well as to the safety of the public. Mobile telephones are used for a range of criminal purposes in these institutions, including commissioning serious violence, harassing victims, intimidating witnesses and facilitating continuing involvement in extremist networks, organised crime and gang activity. Access to mobile telephones is also strongly associated with drug supply, violence and bullying. The 2008 Blakey report¹ 'Disrupting the Supply of Drugs into Prisons' identified the availability of mobile telephones as key to the smuggling of drugs into prisons.

United Kingdom legislation, the *Prisons (Interference with Wireless Telegraphy) Act 2012 (the Act)*, received Royal Assent on 19 December 2012 and will come into force in the United Kingdom this year. A copy of the Act is attached to this consultation as Annex 1. The Act enables prison authorities to be authorised to interfere with wireless telegraphy in order to detect, investigate or prevent the use of electronic communication devices (including mobile telephones) in prisons. In its current state, the Act does not apply to the Bailiwicks of Guernsey and Jersey and therefore, currently, it is an offence in Jersey and Guernsey for any person to interfere or use 'jamming' equipment to prevent the use of wireless telegraphy communications.

However, the Act contains a permissive extent clause enabling it to be extended to either or both of the Bailiwicks of Jersey and Guernsey (or the Isle of Man) on their request. The 'permissive extent clause' does not itself give effect to the Act in the Channel Islands, but merely enables it to be extended at a later date, with appropriate modifications and adaptation, to either or both of the Bailiwicks. The substance of the Act would then be extended by Order in Council and, for example, it is likely that references to the Secretary of State might be replaced by reference to the appropriate Minister in Jersey or the appropriate Department in Guernsey.

The States of Jersey and Guernsey are considering the implications of requesting an extension to the legislation and are seeking views from mobile network operators, before any decision is made. In its role as regulator of the telecommunications sector in the Channel Islands, CICRA (the Channel Islands Competition and Regulatory Authorities) has been asked by the governments of Jersey and Guernsey to co-ordinate this consultation exercise.

¹ The Blakey Review, July 2008

2. Purpose and Structure of the Consultation

Section 3 of this consultation document sets out the legislative background in Jersey and Guernsey for CICRA's role in this consultation and in wider telecoms regulation. Section 4 provides background on the issue that has given rise to this consultation. Section 5 sets out the specific areas on which interested parties are invited to comment.

Interested parties can respond to this consultation in writing, with submissions lodged by hand delivery, post or by email at one of the following addresses:

Suites B1 & B2, Hirzel Court
St Peter Port
Guernsey
GY1 2NH
Email: info@cicra.gg

2nd Floor, Salisbury House
1-9 Union Street, St Helier
Jersey
JE2 3RF
Email: info@cicra.je

All comments should be clearly marked "Prisons (Interference with Wireless Telegraphy) Act - Consultation" and should arrive before Friday, 26 April 2013.

3. Legislative Background

The governments of Jersey and Guernsey have requested CICRA to co-ordinate this consultation exercise given CICRA's contact with mobile network operators and its regulatory functions with respect to mobile telephony and wireless telegraphy.

The legislative basis for this consultation is provided in Jersey by the *Competition Regulatory Authority (Jersey) Law 2001* and the *Telecommunications (Jersey) Law 2002*. In Guernsey, applicable legislation is *The Regulation of Utilities (Bailiwick of Guernsey) Law, 2001*, *The Guernsey Competition and Regulatory Authority Ordinance, 2012*², and *The Telecommunications (Bailiwick of Guernsey) Law 2001*. In addition, there is scope for the States of Guernsey and States of Jersey to give directions to the GCRA and the JCRA respectively.

² This Ordinance provided for the GCRA to be established as a successor to the Office of Utility Regulation (OUR), which had been set up in 2001. The GCRA has taken over the OUR's duties and has added responsibilities in the administration of *The Competition (Guernsey) Ordinance, 2012*.

4. Background to the development of legislation

It is already a criminal offence in the UK to convey a mobile telephone into a prison or to use such apparatus in a prison (without appropriate permission). An Amendment to the *Prison (Jersey) Law 1957* to make similar provision is at the final drafting stage. It is known that illicit mobile telephones have been used to commission crimes from inside Jersey's prison, including the trafficking of drugs to the Island and consequently, thwarting this means of communicating in the criminal fraternity would be of significant public benefit.

In Guernsey, it is currently a disciplinary offence under *The Prison Administration (Guernsey) Ordinance, 1998* for a prisoner to possess any article (which would include a mobile phone) unless authorised by direction of the Prison Governor or the Home Department. In addition, it is a criminal offence under that Ordinance to bring or throw any article into the prison without lawful authority. In the future, *The Prison (Enabling Provisions) (Guernsey) Law, 2010* (currently awaiting approval by the Privy Council) will replace existing prisons legislation and a Departmental Order is being drafted to declare mobile phones and other telecommunications systems to be "prohibited things" under that Law.

The problems posed by mobile phones in prisons were recently identified in the Home Office national drug strategy 2010³, a 2010 Ministry of Justice green paper⁴ and the Home Office organised crime strategy⁵.

The provisions of the Act are designed to create a clear and transparent legal basis on which signal interference equipment can be used within relevant institutions to enable the authorities to find mobile telephones and to disrupt, by means of signal interference equipment, the use of those telephones that cannot be found.

The detection or investigation of the use of such devices may be carried out by collecting 'traffic data' in relation to a communication. The definition of traffic data includes data which is comprised in, attached to or logically associated with an electronic communication and which identifies the person or apparatus or location to or from which the communication is transmitted; identifies apparatus through which the communication is transmitted; or identifies the time at which an event relating to the communication occurs. It does not include the content of the communication.

The Act makes provision for safeguards in order to ensure that, in particular, any undue interference with wireless telegraphy outside of the relevant institution is limited. The Act

³ "Reducing demand, restricting supply, building recovery: supporting people to live a drug-free life" - www.homeoffice.gov.uk/publications/alcohol-drugs/drugs/drug-strategy/drug-strategy-2010

⁴ "Breaking the Cycle: Effective Punishment, Rehabilitation and Sentencing of Offenders" - www.justice.gov.uk/consultations/docs/breaking-the-cycle.pdf

⁵ "Local to Global: Reducing the Risk from Organised Crime" - www.homeoffice.gov.uk/publications/crime/organised-crime-strategy?view=Binary

also provides safeguards regarding the retention and disclosure of information obtained in the exercise of powers under an authorisation. In particular, the Act provides that any information obtained by detecting or investigating the use of electronic communication devices in relevant institutions must be destroyed no later than three months after it was obtained unless the governor or director of the relevant institution authorises its continued retention as being necessary and proportionate on specified grounds. The information obtained may not be disclosed other than to specified persons unless such disclosure is considered as being necessary and proportionate on specified grounds.

5. Areas for comment

Interested parties are invited to comment generally on whether the Act should be extended to Guernsey and Jersey, and specifically on the following questions:

1. What are your views on the possible authorised use of interference equipment to prevent the use of mobile telephones within prison?
2. What are your views on the possible authorised collection, analysis, storage and subsequent destruction of traffic data from mobile telephone users in prison?
3. What might be the possible effects of authorised use of interference equipment on service users resident nearby or passing by outside the prison? Could any unintended effects be mitigated?
4. What might be the possible implications of authorised collection, analysis, storage and subsequent destruction of traffic data from service users resident nearby or passing by outside the prison? Could any unintended collection, etc. be mitigated or prevented?
5. Are there any other technical or operational implications of the proposed legislation? Do you have any other objections or concerns relating to the proposed legislation, the possible use of interference equipment, or the possible authorised collection, analysis, storage and subsequent destruction of traffic data?

Prisons (Interference with Wireless Telegraphy) Act 2012

2012 CHAPTER 20

An Act to make provision about interference with wireless telegraphy in prisons and similar institutions.

[19th December 2012]

BE IT ENACTED by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

1 Interference with wireless telegraphy in prisons etc.

- (1) The appropriate national authority may authorise the person in charge of a relevant institution to interfere with wireless telegraphy.
- (2) An interference with wireless telegraphy authorised under subsection (1) may be carried out only for the purpose of—
 - (a) preventing the use within the institution of an item specified in subsection (3), or
 - (b) detecting or investigating the use within the institution of such an item.
- (3) The specified items are—
 - (a) a device capable of transmitting or receiving images, sounds or information by electronic communications (including a mobile telephone);
 - (b) a component part of such a device;
 - (c) an article designed or adapted for use with such a device (including any disk, film or other separate article on which images, sounds or information may be recorded).
- (4) The interference with wireless telegraphy that may be authorised by virtue of subsection (2)(b) is for the collection of traffic data in relation to an electronic communication and (subject to the provisions of this Act) such an authorisation permits the retention, use and disclosure of that data.
- (5) Conduct to which this subsection applies is lawful for all purposes.
- (6) The conduct to which subsection (5) applies is—
 - (a) interference with wireless telegraphy that—
 - (i) is authorised under subsection (1), and

- (ii) is carried out in accordance with subsection (2) and any direction given under section 2,
 - (b) the retention, use or disclosure of any traffic data, collected as a result of such an interference with wireless telegraphy, which is carried out in accordance with this Act.
- (7) Section 8(1) of the Wireless Telegraphy Act 2006 (requirement for a licence to establish or use a wireless telegraphy station or to install or use wireless telegraphy apparatus) does not apply in relation to anything done for the purposes of carrying out an interference with wireless telegraphy authorised under this section.
- (8) An authorisation under this section must be in writing.

2 Safeguards

- (1) Before the appropriate national authority authorises an interference with wireless telegraphy under section 1 it must be satisfied any equipment that will be used as a result of the authorisation is fit for the purpose.
- (2) Where the appropriate national authority authorises an interference with wireless telegraphy under section 1 it must inform the Office of Communications.
- (3) A person in charge of a relevant institution who is authorised to interfere with wireless telegraphy under section 1 must act in accordance with directions given under this section.
- (4) Where the appropriate national authority authorises an interference with wireless telegraphy under section 1, it must give directions to the person so authorised—
 - (a) specifying descriptions of information to be provided to the Office of Communications;
 - (b) specifying intervals at, or occurrences on, which such information is to be so provided;
 - (c) as to the circumstances in which the use of equipment for the purposes of an interference with wireless telegraphy authorised under section 1 must be modified or discontinued (and, in particular, directions aimed at ensuring that the authorised interference will not result in disproportionate interference with wireless telegraphy outside the relevant institution).
- (5) The appropriate national authority may give such other directions to a person mentioned in subsection (4) as it considers necessary or desirable for the purposes of this Act.
- (6) A direction under this section must be in writing.

3 Retention and disclosure of information obtained under section 1

- (1) Information obtained by virtue of section 1 must be destroyed no later than 3 months after it was obtained unless the person in charge of the relevant institution has authorised its retention.
- (2) The person in charge of a relevant institution may not give an authorisation under subsection (1) unless satisfied—

- (a) that the retention of the information is necessary on one or more of the grounds specified in subsection (8), and
 - (b) that the retention is proportionate to what is sought to be achieved by it.
- (3) Where information is retained under subsection (1) the person in charge of the relevant institution must review, at intervals of not more than 3 months, whether its retention remains in accordance with that subsection.
- (4) If, on a review under subsection (3), the person in charge of the relevant institution is not satisfied that the retention of information remains in accordance with subsection (1), that person must arrange for the information to be destroyed.
- (5) Information obtained by virtue of section 1(2)(b) may be disclosed to—
 - (a) an officer of the relevant institution;
 - (b) an employee authorised for the purposes of this section by the person in charge of the institution;
 - (c) the Secretary of State;
 - (d) if the relevant institution is in Scotland, the Scottish Ministers.
- (6) Information obtained by virtue of section 1(2)(b) may not be disclosed to any other person unless the person in charge of the relevant institution has authorised its disclosure.
- (7) An authorisation under subsection (6) may be given only where the person in charge of the relevant institution is satisfied that—
 - (a) the disclosure is necessary on one or more of the grounds specified in subsection (8), and
 - (b) the disclosure is proportionate to what is sought to be achieved by it.
- (8) The specified grounds are—
 - (a) the interests of national security,
 - (b) the prevention, detection, investigation or prosecution of crime,
 - (c) the interests of public safety,
 - (d) securing or maintaining security or good order and discipline in the relevant institution,
 - (e) the protection of health or morals.
- (9) An authorisation under this section must be in writing.

4 Interpretation

- (1) In this Act—

“the appropriate national authority” means—

- (a) in relation to a relevant institution in England or Wales, the Secretary of State;
- (b) in relation to a relevant institution in Scotland, the Scottish Ministers;

“relevant institution” means—

- (a) a prison in England, Wales or Scotland;
- (b) a young offender institution in England or Wales;
- (c) a young offenders institution in Scotland;
- (d) a secure training centre in England or Wales;

“wireless telegraphy” has the same meaning as in the Wireless Telegraphy Act 2006 and, in relation to wireless telegraphy, “interfere” has the same meaning as in that Act.

(2) In this Act reference to the person in charge of a relevant institution is—

- (a) in relation to a prison, its governor or, in the case of a contracted-out institution in England, Wales or Scotland, its director;
- (b) in the case of a young offender institution or a secure training centre in England or Wales, its governor or, in the case of a contracted-out institution, its director;
- (c) in the case of a young offenders institution in Scotland, its governor or, in the case of a contracted-out institution, its director.

(3) For the purposes of subsection (2) an institution is “contracted-out” if—

- (a) in England or Wales, it is a contracted out prison within the meaning of Part 4 of the Criminal Justice Act 1991 (see section 84(4) of that Act);
- (b) in Scotland, it is a contracted out prison within the meaning of Chapter 2 of Part 8 of the Criminal Justice and Public Order Act 1994 (see section 106(4) of that Act);
- (c) in the case of a secure training centre in England or Wales, it is provided or run in accordance with a contract made under section 7 of the Criminal Justice and Public Order Act 1994.

(4) In this Act “traffic data” means data—

- (a) 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
- (b) which—
 - (i) identifies, or purports to identify, any person, apparatus or location to or from which the communication is or may be transmitted,

- (ii) identifies or selects, or purports to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,
- (iii) comprises signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of the communication,
- (iv) identifies, or purports to identify, the time at which an event relating to the communication occurs, or
- (v) identifies data as comprised in, attached to or logically associated with the communication.

The references in this subsection to a telecommunication system by means of which a communication is being or may be transmitted include, in relation to data comprising signals for the actuation of apparatus, any telecommunication system in which that apparatus is comprised.

- (5) Data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication is not “traffic data” except to the extent that the file or program is identified by reference to the apparatus in which it is stored.
- (6) In this section “telecommunication system” has the same meaning as it has for the purposes of the Regulation of Investigatory Powers Act 2000.

5 Final provisions

- (1) This Act extends to England and Wales and Scotland.
- (2) Her Majesty may by Order in Council provide for this Act to extend with modifications to any of the Channel Islands or the Isle of Man.
- (3) Sections 1 to 4 of this Act come into force on such day as the appropriate authority may by order appoint.
- (4) In subsection (3) “the appropriate authority” means—
 - (a) so far as this Act extends to England and Wales, the Secretary of State;
 - (b) so far as this Act extends to Scotland, the Scottish Ministers.
- (5) An order made under subsection (3) by the Secretary of State must be made by statutory instrument.
- (6) This Act may be cited as the Prisons (Interference with Wireless Telegraphy) Act 2012