HUMAN RIGHTS IN THE MODERN ERA: PRIVACY RIGHTS: A COMMONWEALTH PERSPECTIVE

Colin Nicholls, QC is a barrister at 3 Raymond Buildings Chambers, Gray's Inn in London, UK. He is Honorary Life President of the Commonwealth Lawyers Association and Chair of the Commonwealth Expert Group to Review the Commonwealth Model Law on Computer and Computer Related Crime.

Genevieve Woods is a barrister at 3 Raymond Buildings Chambers, Gray's Inn.

Introduction

The doyens of 20th century human rights declarations and conventions could never have envisaged a world so interconnected as ours, where information is shared globally and instantaneously, and many people live their lives online.

As the digital age expands into homes, between businesses and across borders, legislators are struggling to strike a balance between guaranteeing freedom of expression and protecting privacy, respecting the limits of international jurisdiction, and ensuring that citizens remain safe online. Achieving an effective balance will be one of the great human rights challenges of the 21st century.

The use of bilateral and multilateral mutual legal assistance treaties (MLATs), with their inbuilt protections against violations of the right to privacy and freedom of speech, is an essential part of that process, but as international organised crime escalates and requests for assistance become more numerous and complex, these systems have become overburdened and other solutions are being sought.

The Commonwealth cybercrime and privacy framework

On 20 April 2018, at their meeting in London, 53 Heads of Commonwealth Governments, including the Heads of 31 Small Commonwealth and Island States, unanimously adopted a landmark *Commonwealth Cyber Declaration* committing themselves to:

- A cyberspace that supports economic and social development and rights online;
- Building the foundations of an effective national cyber security response; and
- Requiring cyber security frameworks to promote stability in cyberspace through international cooperation.

The Declaration, which has been described as *"the world's largest and most geographically diverse inter-governmental commitment on cybersecurity cooperation"*[1], followed immediately after the UK Government's announcement to pledge up to £15 million to help Commonwealth countries strengthen their cybersecurity capabilities. It was accompanied by an Implementation Plan for the Period 2018—2020, in which the Heads of Governments agreed to examine and assess their cybersecurity frameworks and to determine their capacity needs.[2]

Commonwealth countries have long recognized the importance of the right of the public to access information held by the government and the need to protect the privacy of individuals whose personal information is held by public or private organisations. Between 2002 and 2005, Law Ministers adopted three inter-related bills to assist Commonwealth member countries, which had yet to enact laws providing for access to information: *The Model Privacy Bill (2002)*; *The Model Freedom of Information Bill (2002)*; and *The Model Bill on the Protection of Personal Information (2005)*. Each of them draws largely from the core principles set out in the OECD Privacy Guidelines 1980, updated in 2013[3]

The Commonwealth also has *The Harare Scheme*[4] an established framework of mutual legal assistance, updated in 2011 to include preservation of computer data, interception of telecommunications and covert electronic surveillance. The Scheme has clear built-in safeguards to protect the sovereignty of Commonwealth states and the privacy of Commonwealth citizens. The Commonwealth also has in place the *Commonwealth Network of Contact Persons*, which provides investigators and prosecutors with practical and legal advice and enhances informal cooperation; the *Commonwealth Cybercrime Initiative*, a consortium of 35 international organisations including Interpol, the Council of Europe, UNODC, and the Commonwealth Telecommunications Organisation, which provides member countries with technical assistance on cybercrime and cybersecurity capacity building on request.

In 2011, Law Ministers adopted *The Commonwealth Model Law on Computer and Computer Related Crime*, which is currently being reviewed by a Commonwealth Expert Group, and provides a legislative framework of cyber related offences based upon the Council of Europe's *Convention on Cybercrime (The Budapest Convention)*[5], the Preamble of which specifically recognises:

"… the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy" and *"the right to the protection of personal data…"*

The *Budapest Convention* has been ratified or acceded to by 61 states. Eight Commonwealth countries[6] are Parties to it and others have introduced legislation

based upon it. It sets out an MLA framework similar to the Harare Scheme, with provision for states to impose restrictions ensuring that data disclosed is not used for purposes other than those contained in the MLA request.

Mutual Legal Assistance: the need for change

The Commonwealth privacy framework is comprehensive and like the *Budapest Convention* is subject to review, but as technology has advanced and requests for MLA assistance have soared, the bureaucracy involved in responding to requests has led to delays which are unacceptable if the destruction of incriminating data is to be avoided, and serious crime, particularly economic and international organised crime, is to be effectively investigated and prosecuted.

In 2013, a UN study found that the MLA process takes, on average, 150 days from request to response.[7] In April 2017, Google noted in its *Transparency Report* that it received 45,549 government requests for user data in the second half of 2016 of which 31,000 (approximately 70%) were from non-US governments. Not surprisingly it called for a more efficient legal process than the current MLA treaties.[8]

The Commonwealth model bills on privacy and freedom of information are at least twelve years old and a Working Group is currently reviewing the *Commonwealth Model Law on Computer and Computer Related Crime*. Investigators and prosecutors are challenging the effectiveness of MLA treaties and seeking other solutions. The US has enacted and the UK is enacting legislation to make it easier for law enforcement agencies to obtain electronic evidence, including emails and documents stored on the Cloud, and they are negotiating an international cooperation agreement to give it effect. Similarly, a European Union instrument that would allow Member States to obtain data directly from companies in other Member States is making its way through the European Parliament, although the UK will need to forge fresh agreements with Member States post-Brexit.[9]

Two recent cases, one in the US and one in the UK, illustrate the difficulties which have arisen in resolving issues of territoriality in pre-Internet age statutes and which demonstrate the need for legislative intervention.

The US Solution: The Microsoft Litigation and the CLOUD Act

On 14 July 2016, in *Microsoft v US 829 F 3d* (2d Cir. 2016), the Court of Appeals for the Second Circuit in a majority judgment allowed an appeal by Microsoft against a decision of the United States District Court, which had held Microsoft in contempt for failing to comply with a warrant requiring it to produce the contents of a US customer's email account stored in Ireland.

The warrant had been issued under the *Stored Communications Act, 18 USC 2701 ("the SCA 1986")*; a pre-Internet age statute. The Court of Appeals accepted Microsoft's argument that the issue of the warrant constituted an unlawful extraterritorial application of the SCA 1986, and held that in the absence of express contrary intention in the statute, warrants under the SCA could only apply within the jurisdiction.

The US Government obtained leave to appeal to the US Supreme Court, but on 23 March 2018 the President signed the *Clarifying Lawful Overseas Use of Data Act (the CLOUD Act)*, which amended the SCA 1986 by expressly providing that the Act had extraterritorial application subject to certain conditions. The Government obtained a fresh warrant under the new law and the issue under appeal being no longer moot, the Supreme Court declined to consider the original appeal.

The CLOUD Act created an alternative route to that provided by MLA treaties, empowering the President to make 'executive agreements' with 'qualifying' foreign governments enabling them to obtain requested data of their citizens in a streamlined manner. Governments, which are parties to such agreements, can issue orders which are binding on US providers after the orders have been approved by their domestic judiciaries and without requiring judicial approval in the United States. The 'executive agreements' are confined to 'serious crime and terrorism' and can only be made if the Attorney General and Secretary of State certify that among other things, the foreign government provides 'robust substantive and procedural protections for privacy and civil liberties' and that it has adopted procedures to 'minimize the acquisition, retention, and dissemination of information concerning United States persons."[10]

The UK Solution: Overseas Production Orders

On 27 June 2018 the UK Government introduced in the House of Lords the *Crime (Overseas Production Orders) Bill ("OPO")*, which, if enacted, will enable UK law enforcement agencies to apply to a domestic court for an order authorising them to obtain electronic data directly from service providers based outside the UK. As with the CLOUD Act, an order may only be made where an agreement, in this case called an 'international agreement' is in place with the country where the provider is based.

The order is limited to indictable offences and terrorist investigations. It must specify the data that is being sought, and the judge must be satisfied that the data is likely to be of substantial value to the proceedings or the investigation, and that its production will be in the public interest. It may also include a requirement that no other person shall be informed of its existence. The Bill provides that the server *'and any person affected'* by the order may apply to the domestic court for all or part of the order to be revoked, but makes no provision for the executing state to make any objection.

At the time of writing, the Bill has passed the Report Stage in the House of Lords and after a Third Reading, will be considered by the House of Commons. The Government has asserted that the Bill is compatible with the *Human Rights Act 1998*[11], stating that although it overrides Articles 8 and 10 of the European Convention on Human Rights, *"these intrusions into ECHR rights can be justified as necessary in a democratic society for the prevention of disorder and crime and in the interests of national security and public safety, and are proportionate in light of the requirements that must be*

"There is no question that legislative changes are needed to bring prosecutorial powers up to date with new technology and to supplement the current system of mutual legal assistance. However, the risks to privacy and sovereignty in creating alternative frameworks are apparent and there are no easy answers."

met before a judge can make an overseas production order, and the other safeguards set out in the Bill."

While the Bill includes safeguards; like the CLOUD Act, it has raised serious human rights concerns. The Bill contains provisions protecting personal, confidential and journalistic data, and the allows persons affected by the order to apply for it to be revoked or amended, but the process of review is one-sided and places considerable trust in the law enforcement agencies of the requesting state. Executing states have played a vital role in safeguarding citizens' rights in the application of existing MLATs, but will have no power to scrutinise OPOs.

A judicial solution: KBR v SFO

On 6 September 2018, while the OPO was progressing though Parliament, the UK High Court handed down its judgment in the case of *KBR v SFO*, holding that section 2(3) of the *Criminal Justice Act 1987*, a pre-Internet statute which grants the Serious Fraud Office (SFO) power to compel the production of documents, can have extraterritorial application.

The case concerned the validity of a '*section 2 notice*' issued by the SFO which required KBR Inc., the USA-based parent company of KBR Ltd, which was accused of making corrupt payments, to hand over documents held outside the UK. The notice had been served on a representative of KBR Inc whilst she was in the UK.

The court held that the SFO may compel the production of documents by an overseas company *"when there is a sufficient connection between the company and the jurisdiction"* (at [71]) and that KBR Inc. had sufficient connection simply by authorising payments made by its subsidiary, KBR Ltd, which had originated in the UK.

Although KBR argued that giving section 2 extraterritorial effect would improperly circumvent the statutory mutual legal assistance framework and the safeguards put in place to protect and respect international sovereignty, the court held that the section 2 powers could be used as an alternative to MLA and that this was in the public interest in order to combat cross-border crime in the internet age. As Gross LJ stated: *"… The SFO's business is "top end, well-heeled, well-lawyered crime…" By their nature, most such investigations will have an international dimension, very often involving multinational groups conducting their business in multiple jurisdictions… It follows that the documents relevant to the investigation of a UK subsidiary of such a group may well be spread between the UK and one or more overseas jurisdictions. … there would be a very real risk that the purpose of section 2(3) would be frustrated… if, as a jurisdictional bar, the SFO was precluded from seeking documents held abroad from any foreign company…. There is, accordingly, an extremely strong public interest in the extraterritorial ambit of section 2(3)…"* [68].

There remain difficult questions about the logistics of enforcing section 2 notices on persons abroad and the High Court decision may yet be appealed, but the prospect of the SFO issuing section 2 notices threatening overseas corporations or individuals with fines or imprisonment for non-compliance may be regarded as a drastic incursion into international comity and could lead to the erosion of states' goodwill.

As in the *Microsoft Case*, the ruling in the *KBR Case* demonstrates the difficult issues which can arise in the interpretation of pre-Internet statutes and which may only be definitively resolved by the legislature. The SFO's section 2 powers are not subject to the MLA safeguards provided by the *Budapest Convention* and the Harare Scheme, which were carefully drafted to satisfy the need to balance law enforcement with respect for the sovereignty of foreign states. Instead, a domestic law enforcement agency has been empowered unilaterally to act internationally, seizing overseas materials and threatening foreign corporations with criminal sanctions without seeking the consent of the relevant state.[12]

Conclusion

There is no question that legislative changes are needed to bring prosecutorial powers up to date with new technology and to supplement the current system of mutual legal assistance. However, the risks to privacy and sovereignty in creating alternative frameworks are apparent and there are no easy answers.

The *OPO Bill* and the *CLOUD Act*, together with the proposed *European Production Order*, are important steps towards creating an effective international information-sharing scheme, but they are limited and lack the global response that is required. The pool of participating states is rightly restricted to those countries which are able to satisfy the respective governments that they are suitable treaty partners by demonstrating their compliance with the safeguards provided by MLATs and international agreements such as the *Budapest Convention*. However, as the UN warned in 2013, these emerging networks of selected countries are limited in scope and are not always well suited to the global nature of cybercrime.[13]

Small and developing Commonwealth countries may struggle to persuade the US, the UK, and the European Union to agree to their participation in agreements of the types proposed, in which case they must continue to use the current system of MLA, move towards the creation of regional networks to expedite information-sharing, or be tempted to launch challenges similar to those in the *Microsoft* and *KBR* cases.

A timely review of the relevant Commonwealth Model Laws, together with other Commonwealth schemes, may help to provide a solution to one of the most pressing human rights problems of the 21st century – the protection of citizens online and of their online rights.

References:

[1] http://thecommonwealth.org/media/news/commonwealth-takes-strong-stance-against-cybercrime-landmark-declaration

[2] https://www.gov.uk/government/news/uk-commits-to-a-safer-commonwealth-in-cyber-space

[3] The OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data http://www.oecd.org/sti/ieconomy/49710223.pdf, Law Ministers approved two further model laws in 2002: The Commonwealth Model Law on Electronic Evidence, and The Commonwealth Model Law on Electronic Transactions

[4] The Commonwealth Scheme Relating to Mutual Legal Assistance in Criminal Matters in the Commonwealth.

[5] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[6] Australia, Canada, Cyprus, Malta, Mauritius, Sri Lanka, Tonga, UK.

[7] https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[8] Transparency Report.google.com; znet.com

[9] http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/621844/EPRS_BRI(2018)621844_EN.pdf

[10] CLOUD Act §105

[11] https://publications.parliament.uk/pa/bills/lbill/2017-2019/0113/18113en.pdf pg 8

[12] See further: Masri v Consolidated Contractors Int (UK) Ltd (No. 4) [2009] UKHL 43; [2010] 1 AC 90, per Lord Mance at [10], referred to by Gross LJ in the KBR Case at [26].

[13] The UN Comprehensive Study on Cybercrime 2013 at xxvi, https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html