Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comment

It wasn't all white light before *Prism*: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe

Micheál O'Floinn

School of Law, University of Southampton, UK

Keywords:
Cybercrime
Transnational access
Data
Investigations
Cybercrime Convention
Council of Europe
T-CY

ABSTRACT

This is a brief comment on a meeting held at the Council of Europe in Strasbourg, which discussed ways of improving transnational access to data by law enforcement through the Cybercrime Convention. In particular, the possible introduction of a new protocol, and a guidance note on art. 32(b), were considered. It is argued that there are serious concerns with both proposals. Moreover, the meeting revealed a surprising lack of knowledge as to current levels of cooperation between law enforcement and foreign service providers.

1. Introduction

The aftermath of the *Prism* and *Tempora* revelations has rightly generated uproar concerning the legality of law enforcement's transnational access to data, and few had even realised that such mass surveillance was possible under existing US and UK legislation.[1] The lack of appreciation of what is done under extant law can be partly explained by a lack of knowledge as to what the intelligence agencies actually do in their day-to-day work. Less explicable, however, is the widespread lack of appreciation of more overt tools used by Law Enforcement Agencies (LEAs) to gain access to data stored both domestically,[2] but also abroad. Authoritative writers on international law have long

[1] There are exceptions here. See the excellent report by Caspar Bowden and others for the European Parliament "Fighting Cyber Crime and Protecting Privacy in the Cloud." (2012) Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/study_cloud_/study_cloud_en.pdf. Supposedly, the tapping of transatlantic cables by GCHQ was authorised by interception warrants, and over 100 certificates issued under s. 8(4) of the Regulation of Investigatory Powers Act 2000 (RIPA). Privacy International has filed a complaint concerning, *inter alia*, the compatibility of such warrants with art. 8 ECHR, before the Investigatory Powers Tribunal: www.privacyinternational.org/press-releases/privacy-international-files-legal-challenge-against-uk-government-over-mass.

[2] Much of the critique of the Draft Communications Data Bill, for example, seemed to be oblivious to the existing police powers for acquiring communications data under RIPA.

0267-3649/$ – see front matter © 2013 Micheál O'Floinn. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2013.07.015

considered it unthinkable for LEAs to directly approach an individual in a foreign territory for information,[3] and some States continue to regard it as a criminal offence.[4] But the times they are a-changin'. LEAs routinely request—and are provided with—data from foreign service providers, without formal inter-State process such as mutual legal assistance (MLA), and there is no need for Snowden to tell us this. Ebay and Facebook have dedicated portals for facilitating such exchanges,[5] and providers such as Hotmail, Google, Microsoft and Facebook speak openly about their 'voluntary' and 'cooperative' relationship with UK law enforcement.[6] If these providers were based in the UK, access to communications data could be achieved within seconds via a secure extranet and an internally authorised LEA request (e.g. there is no need for a court order).[7] What is of note, however, is that such requests are also being answered transnationally without the providers being under any legal compulsion to do so; the RIPA request may well have all the T's crossed and I's dotted, but it has no binding force abroad.

It is against this backdrop that a meeting was held at the Council of Europe in Strasbourg to discuss possible ways of improving transborder access to data by law enforcement, through the Cybercrime Convention. The background to this meeting is that in 2011 the Cybercrime Convention Committee (T-CY) established an "ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows." It tasked the Transborder Group (TG) with developing an instrument (e.g. an amendment to the Cybercrime Convention, a Protocol, or recommendation) to further regulate transborder access to data and data flows, and the use of transborder investigative measures on the Internet and related issues.

In December 2012, the report of the TG was adopted by the T-CY, and a number of interested stakeholders and experts were invited to discuss it in a hearing at the Council of Europe on June 3rd 2013. The meeting was well attended by the private sector (e.g. Google, Microsoft, Paypal, Symantec, Leaseweb), NGOs, Parties to the Convention, representatives of the T-CY, observer countries and organisations, as well as some academics (myself included) and other interested parties.

The particular recommendations of the TG which were discussed concerned: 1. A new Guidance Note on art. 32 of the Cybercrime Convention, and 2. A new Additional Protocol to allow for "additional possibilities for transborder access to data." Their recommendations on the possible content of both were analysed in some detail on the day, and below are some selected observations on both issues.

2. A Guidance Note on art. 32

Art. 32 of the Cybercrime Convention deals with two different types of transborder access to data by Parties to the Convention: the first is uncontroversial and provides that a Party can gain access to publicly available stored computer data (e.g. a LEA reading a public webpage hosted in another country); the second allows a Party, using a computer system in its territory, to access "stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party."[8]

This latter provision is arguably the most controversial provision in the Convention, and is widely known to be one of the main reasons for Russia's non-ratification. The discussions on June 3rd suggested there was good reason for some hesitation regarding this provision, because the various meanings of 'consent' which arise for consideration had many heads spinning not long into proceedings. Participants began speaking past one another with much confusion stemming from uncertainty as to how data protection obligations intersected with art. 32(b). Some (such as the representatives from the European Commission and the T-PD[9]) could not see how a service provider in the EU could respond directly to a foreign LEA request, without the data subject's specific consent to do so, or other lawful authority like an MLAT. Others (such as the representatives from the International Chamber of Commerce and Symantec) could not see why this was such a point of contention since it is a type of interaction occurring routinely; they pointed to customers' agreement to the terms of service, which normally provide for such disclosure to law enforcement.[10] The proposed guidance note did not help matters with contradictory

[3] FA Mann, 'The Doctrine of International Jurisdiction Revisited After Twenty Years' in M Reisman (ed), *Jurisdiction in international law* (Aldershot: Ashgate 1984), footnote 82.

[4] Report of the Transborder Group on 'Transborder access and jurisdiction: what are the options?' (2012), para. 118. Presumably, the offence is committed by the investigating officer, in the foreign territory, as soon as the individual receives the enquiry.

[5] See lers.corp.ebay.com/AIP/portal/home.do and www.facebook.com/records.

[6] See e.g. the first report of Joint Committee on the Draft Communications Data Bill (2012), paras. 230–233. Available at: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf.

[7] Although there is some difficulty in defining these different service providers from a regulatory perspective, which could impede access. See M. O'Floinn and D. Ormerod 'Social networking sites, RIPA and criminal investigations' (2011) 10 Criminal Law Review 766.

[8] For an excellent analysis of this provision in this context, see Ian Walden, 'Accessing data in the cloud: The long arm of the law enforcement agent', in S. Pearson and G. Yee (eds) *Privacy and security for cloud computer* (2013, Springer-Verlag, London).

[9] The Council of Europe's Consultative Committee of the Convention for the Protection of Individuals Regarding Automatic Processing of Personal Data.

[10] A recent survey of standard terms and conditions used by cloud service providers revealed that, almost without exception, they reserved the right to disclose customer data to law enforcement in specified circumstances. These circumstances ranged from requiring a court order, to acting in the company's best interests. See S. Bradshaw, C. Millard and I. Walden, "Contracts for Clouds: A Comparative Analysis of Terms and Conditions for Cloud Computing Services" *International Journal of Law and Information Technology*, 19 (2011) 3.