COMPUTER LAW & SECURITY REVIEW 000 (2018) 1–7

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

'The Sky is Falling!' – Responses to the 'Going Dark' problem

*Ian Walden**

Centre for Commercial Law Studies, Queen Mary University of London, UK

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Encryption
Digital forensics
Law enforcement access
Budapest Convention
Cybercrime
Export control
Lawful intercept
Hacking

ABSTRACT

The shared concern expressed in the two quotes below is that modern technologies provide criminals with a capability to evade investigation. This comment piece examines some of the policy and legal options available to governments and law enforcement agencies to try to address this concern. While accepting the claim that this phenomenon represents a real challenge to law enforcement agencies, we currently have insufficient evidence to show the true extent of the problem. What this piece does not accept is the implication contained in the quotes, and often made explicit by others, that the use of encryption represents a fundamental and irreversible shift in the balance of power between criminals and their investigators from what previously prevailed. Such claims tend to lack historical perspective, which is one of the themes of this 200th issue of *Computer Law and Security Review*.

> Encrypted communications that cannot be intercepted and locked devices that cannot be opened are law-free zones that permit criminals and terrorists to operate without detection by police and without accountability by judges and juries.
>
> *Rod J. Rosenstein, US Deputy Attorney General* (October 2017)

> The inability to gain access to encrypted data in specific and targeted instances … is right now severely limiting our agencies' ability to stop terrorist attacks and bring criminals to justice.
>
> *Amber Rudd, Home Secretary* (August 2017)

As well as the year in which this journal was first published, 1985 has also been described as the year when digital forensics first emerged as a discipline.[1] Digital forensics has been defined in the following terms:

> *the process by which information is extracted from data storage media…, rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings.*[2]

Extracting data generates a range of problems for investigators, many of which require not only specialist skills and techniques, but also an appropriate legal framework to support such activities. This comment piece examines one of those 'data problems', the 'going dark' or protected data problem.[3]

While 'encryption' is the commonly used term to describe the technological effect of data 'going dark', there are

* Correspondence to: Centre for Commercial Law Studies, Queen Mary University of London, 67-69 Lincoln's Inn Fields, London WC2A 3JB, UK.
E-mail address: i.n.walden@qmul.ac.uk

[1] Pollitt, M., 'A history of digital forensics', pp. 3–15, in *Advances in Digital Forensics* VI, Chow, K-P and S. Shenoi (eds), Springer, 2010.
[2] Forensic Science Regulator, No. 26, October 2015.
[3] For an examination of other data problems, see Chapter 4 in Walden, I., *Computer Crimes and Digital Investigations*, 2nd ed., OUP, 2016.

https://doi.org/10.1016/j.clsr.2018.05.013
0267-3649/

numerous techniques that protect data from being accessed, extracted and interpreted by forensic investigators. Broadly, these operate either at the device level, controlling access to the device, medium or equipment on which forensic material may be held; or on the data itself, transforming it into unintelligible ciphertext. Both represent obstacles to investigators, but operate at different levels in terms of protecting data. Protection measures may also be applied at different points within the life cycle of data, implemented by different persons and for differing reasons. While this piece focuses on encryption, this broader landscape should be kept in mind.

The aim of this comment piece is to contribute to a public debate in the UK that sometimes can appear highly polarised; stuck between law enforcement demands for something to be done and claims by others, particularly those in the technical community, that nothing can, or should, be done. It examines a range of options available to law enforcement, primarily from a UK perspective and in light of recent developments, including some of the human rights aspects. This is by no means a new debate, nor the first articulation of options;[4] however, as illustrated by Amber Rudd's comments (since resigned!), it is becoming re-energised in the UK. The options are not intended to be comprehensive; focusing instead on those considered the most significant. They are also presented in no particular order of suitability, effectiveness and (certainly not) desirability. The hope is that greater awareness of the spectrum of approaches can help inform the debate by challenging the binary perspective generally voiced by politicians, which can sometimes sound like the proverbial broken record!

1. Option 1: criminalise supply, possession or use

A first option is to criminalise the supply, possession or use of cryptographic technologies. Within this option, three distinct approaches can be identified.

First, criminalising the supply or possession of encryption technologies as a tool and facilitator of criminal conduct. Such provisions are a feature of cybercrime statutes, specifically the Council of Europe Convention on Cybercrime ('Budapest Convention'), at article 6, and implemented into UK law by s. 3A of the Computer Misuse Act 1990). Such measures are designed to prevent crime by disrupting the availability of tools that comprise part of the supply chain that results in criminality. A key problem with this approach is distinguishing legitimate from unlawful uses, since encryption technologies will usually be designed for general application and therefore evidencing the appropriate *mens rea* of either the supplier or possessor often proves a high threshold to meet. Prosecuting the supply of such tools in respect of copyright piracy of computer games and broadcast content, for example, is relatively rare and generally uncontroversial.[5] Conversely, the potential for abuse in respect of possession offences is most starkly illustrated by the recent actions of the Turkish government in pursuing and prosecuting suspects of involvement in the 2016 failed coup on the basis that they had downloaded and used the 'ByLock' app, which is an encrypted online messaging application, rather than the content of what was communicated.[6]

While dual-use is the challenge for criminalising encryption technologies, dual-use is also the basis for export control laws, which constitute a regulatory regime designed to govern the export of technologies that have both military and civil application.[7] The primary objective is to prevent sophisticated technologies falling into the hands of the state's enemies that could then be used against it. The regime regulates through licensing or prohibits the export of specified products, in both tangible and intangible form,[8] to specified countries. A breach of the regulations is generally a criminal offence. However, as illustrated by *Bernstein v U.S. Department of Justice*,[9] such rules can be vulnerable to challenge on grounds of being a prior restraint of free speech. Some jurisdictions, such as Russia and China, also regulate the importation of encryption technologies, in order to control their deployment for criminal purposes.

A third approach is to criminalise the use of encryption in connection with criminal conduct, either as a distinct offence or as an aggravating factor when assessing the seriousness of the offence. In the US state of Virginia, for example, use of encryption is "an offense which is separate and distinct from the predicate criminal activity".[10] Under French law, use of encryption in connection with an offence, can raise the status of the criminality to an aggravated crime, attracting significantly enhanced sentences.[11] In the UK, the Sentencing Council has stated in guidelines that the 'deliberate use' of encryption to facilitate the commission of a terrorism offence, or impede detection, should be an aggravating factor in sentencing decisions.[12]

2. Option 2: compulsory disclosure

Under this approach, the person in possession of the protected data, or the 'key' capable of converting the ciphertext back to plaintext, is placed under a legal obligation to disclose either

[4] In the US, see Kerr, O., and B. Schneier, *Encryption Workarounds*, March 2017, available at https://ssrn.com/abstract=2938033 and Woods, A., *Encryption Substitutes*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1705 (July 17, 2017), available at https://lawfareblog.com/encryption-substitutes.

[5] E.g. *Gilham (Christopher Paul)* [2009] EWCA Crim 2293.

[6] See the European Court of Human Rights judgement in *Mehmet Hasan Altan v Turkey* (No. 13237/17), 20 March 2018.

[7] E.g., Council Regulation No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. OJ L 134/1, 29 May 2009, Category 2, Part 5 'Information Security'.

[8] Ibid., at 2(2)(iii) Export includes the "transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community;".

[9] 945 F. Supp. 1279 (N.D. Cal. 1996).

[10] Computer Crime Act at Sections 18.2–152.15: 'Encryption used in criminal activity'.

[11] Penal Code 132-79 (aggravated crime), with an uplift from 20 to 30 years.

[12] Sentencing Council, *Terrorism Offences: Definitive Guideline*, at (27 April 2018).

Please cite this article as: I. Walden, 'The Sky is Falling!' – Responses to the 'Going Dark' problem, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.05.013