Council of the European Union Questionnaire: Encryption – Home Office Responses

1. How often do you encounter encryption in you operational activities and while gathering electronic evidence in cyber space in the course of criminal procedures?

Almost always.

2. What are the main types of encryption mostly encountered during criminal investigations in cyber space?

We encounter all types of encryption. For online encryption this includes email (PGP/GPG), SFTP, HTTPS, SSH Tunnelling, TOR, P2P/12P, e-data stored in the cloud and e-communications. For offline encryption this includes encrypted digital devices such as mobile phones and tablets etc and encrypted applications such as TrueCrypt, VeraCrypt, DiskCryptor etc.

3. Under your national law, is there an obligation for the suspects or accused, or persons who are in possession of a device/e-data relevant for the criminal proceedings, or any other person to provide law enforcement authorities with encryption keys/passwords? If so, is a judicial order (from a prosecutor or a judge) required? Please provide the text of the relevant provisions of your national law.

Yes

Please Specify:

Part III of the Regulation of Investigatory Powers Act 2000 (RIPA) enables a notice to be served on a holder of encrypted information requiring them, where necessary and proportionate, to put that information into an intelligible form where it has been lawfully obtained by a public authority.

This may include, for example, requiring a suspect in a criminal investigation to provide the password to their mobile phone where it has been seized by the police.

The use of these powers is subject to strict safeguards. Permission to require that protected information is put into an intelligible form may only be granted where necessary and proportionate. These powers can only be exercised in the interests of national security, to prevent or detect crime, or in the interests of the economic well-being of the UK. In addition, these powers must not be used where the person with the appropriate permission can obtain possession of the protected information in an intelligible form without the giving of a notice.

A person may only serve a notice in relation to protected information if they have been granted permission by a relevant authority. Public authorities may obtain appropriate permission from a person holding judicial office where protected information has been obtained under a warrant issued by such a person. Such permission might be granted, for example, in relation to a production order obtained

from someone holding judicial office under the Police and Criminal Evidence Act 1984.

Where protected information is likely to be, or has been, obtained in consequence of an authorisation under Part III of the Police Act 1997 (authorisation of otherwise unlawful action in respect of property) appropriate permission for giving a notice may be obtained from an authorising officer within the meaning of that Act.

The Police, National Crime Agency, Her Majesty's Revenue and Customs and members of HM Armed forces have appropriate permission, without requirement for permission to be granted by a judicial authority or Secretary of State, in relation to protected information in certain circumstances. This is the case where that information has been obtained by the exercise of a statutory power and is not information obtained under a warrant issued by the Secretary of State or a person holding judicial office, or an authorisation under Part III of the Police Act 1997, or information obtained by the intelligence agencies. For example, this could be in relation to information obtained under section 19 of the Police and Criminal Evidence Act, which relates to a constable's general powers of seizure.

4. Under your national law, are service providers obliged to provide law enforcement authorities with encryption keys/passwords? If so, is a judicial order (from a prosecutor or judge) required?

No.

Please specify:

5. Under your national law, is it possible to intercept/monitor encrypted data flow to obtain decrypted data for the purposes of criminal proceeding? If so, is a judicial order (from a prosecutor or a judge) required?

No.

Please Specify:

Section 17 of the Regulation of Investigatory Powers Act 2000 prevents intercepted material from being used as evidence in legal proceedings.

6. What are the main issues typically encountered while interception/monitoring encrypted data flow in order to obtain decrypted data?

Section 17 of the Regulation of Investigatory Powers Act 2000 prevents intercepted material from being used as evidence in legal proceedings.

7. What other approaches/techniques do you use for decrypting encrypted e-evidence and securing it so that it is admissible as evidence in the criminal proceedings? Do your authorities use eg the services of foreign companies or assistance from Europol for the purposes of decryption?

Brute force attacks are done with custom dictionaries.

8. Do you consider that your current national law allows sufficiently effective securing of evidence when encrypted? If not, why?

Please Specify:

This response is not related specifically to the securing of evidence given intercepted material cannot be adduced as evidence under UK law. However, encryption is now almost ubiquitous and is the default setting for most IT products and online services. The UK Government recognises the importance of encryption, which ensures companies and individuals can go about their business online safely and securely. But this same technology can also be used - easily and cheaply - by terrorists, paedophiles and other criminals who would seek to do the public harm. As the heads of our security and intelligence and law enforcement agencies have consistently made clear, the problems posed by the use of encryption are real and increasing.

We remain committed to taking a collaborative approach with industry to ensure that law enforcement agencies can access the content of criminals' communications to assist investigations and prevent criminal activity.

In UK law, whether a particular company can be required to remove encryption turns on what is reasonably practicable and technically feasible for them to do. The Investigatory Powers Bill, which is currently being scrutinised by the UK Parliament, provides a mechanism through which Government can undertake the sorts of technical discussions necessary with companies to determine this in relation to their particular system architecture. The Bill would only require operators to remove encryption where it is reasonably practicable and technically feasible to do so – subject to strict safeguards.

However, this does not mean UK law will enable law enforcement to obtain the information they need in unencrypted form in all cases. Undoubtedly, there will be companies and systems where the provisions of UK law do not allow the authorities to require the removal of encryption. Encryption will therefore remain a significant challenge to the UK authorities.

9. What main issues do you typically encounter when seizing encrypted evidence and decrypting it?

Technical – having the relevant technical expertise to make progress.

10. In your view, will measures in this regard need to be adopted at EU level in the future?

We recognise that this remains a complex area. The UK remains committed to taking a collaborative approach with international partners and industry so that

encryption can continue to keep to keep people’s data safe and secure, whilst not allowing serious criminals to operate beyond the reach of law enforcement.

OSCT, Home Office, October 2016