Encryption, the Challenges for Criminal Investigation Authorities and the Role of Human Rights Guarantees

Sarah Summers

> *'The debate on investigatory powers, as I discovered when I was asked by Parliament to report on it, is addictive to some and toxic to everybody else. Securocrats seek access to innocent communications, while privacy advocates warn darkly of dystopia. The rest of us tend to be bored, confused and generally defeated by it all.'*[1]

I. Introduction

Christian Schwarzenegger would resist being categorised, I am sure, as a securocrat or a privacy advocate. His long enthusiasm for all cyber-crime related-matters means, though, that he would probably also resist Anderson's characterisation of the response to the regulation of investigatory powers as boredom, confusion or defeat. That, at least, is what I am counting on in my decision to select this topic as my contribution to this collection of essays in his honour.

The impact of privacy concerns raised in the aftermath of the Snowden revelations has extended beyond the confines of national security.[2] Such concerns have become increasingly evident in the law enforcement context. Police and prosecutorial practices, in context of big data and bulk collection of data, have given rise to considerable controversy.[3] At the centre of this discussion is essentially consideration of the manner in which police (or prosecutorial) surveillance and investigations ought to be regulated. This article focuses on just one aspect of such investigations, the challenge of encrypted content. The article will first illustrate the technical challenges and the legal response to these before going on to consider the (in)adequacy of the European constitutional-type protections regulating the activities of the investigation authorities in this context.

1 Anderson QC, The Investigatory Powers Bill is Still a Work in Progress, The Telegraph, 2 March 2016.

2 Snowden, Permanent Record, New York 2019.

3 Justice, Freedom from Suspicion: Building a Surveillance Framework for a Digital Age, London 2015.

II. Encryption

Encryption is 'the process of transforming some text known as the plain text into a form which cannot be read by anyone who does not have knowledge of the mechanisms used to carry out the encryption. The transformed text is known as the cipher text.'[4] Essentially, encryption does not prevent the interception of communications but prevents the interceptor from accessing the content of the message. Encryption is obviously closely related to security. Encryption poses difficulties for law enforcement because intercepted data is unreadable or because even if the investigating authorities have seized a device – such as a mobile phone or computer – they are powerless to access the content without the relevant password. Difficulties in forcing the owner of a mobile device or computer to reveal his or her password (either because the whereabouts of a suspect is unknown or because the suspect refuses to disclose the password) have led to law enforcement bypassing suspects and approaching communications operators and tech companies in order to secure access to the content of the device.

These issues were are well illustrated by the San Bernardino case. In a well-publicised dispute between Apple and the FBI, the FBI sought to compel Apple to assist in decrypting the data on the iPhone of one of those responsible for carrying out an attack in San Bernardino, California, which led to the deaths of 14 people. The FBI had received permission to search the phone but had not been able to guess the password to unlock it. In iOS devices, most files are encrypted using a combination of a secret key stored on the device and the user's passcode. Data may be wiped after too many incorrect attempts at getting the password. The FBI therefore applied for a court order that Apple be compelled to assist it by removing protections from the operating system in order to allow it to make unlimited number of password guesses without the data being erased. Apple sought to resist the request on the basis that it would undermine the security of their products by leaving customers vulnerable to unlawful interference with their communications. The US Government subsequently dropped the legal action after the FBI successfully managed to access the data stored on the iPhone. This was just one of a number of cases in which investigation and prosecution authorities had requested assistance from Apple.

Such cases reflect the fact that tech companies, worried by privacy invasion by governments and the resulting potential for loss of business, have jettisoned their policies of quiet cooperation with governments and law enforcement and have started championing their independence and commitment to consumer privacy. Companies such as Apple and Google have made efforts to strengthen encryption and have designed encryption strategies, which they claim makes it extremely difficult for them to access the data held on phone. This type of encryption is increasingly seen to pose a challenge to the existing warrant regime and represents an obvious obstacle to law enforcement authorities, which are seeking access to content on such devices by rendering warrants to compel such companies to produce content ineffective.

III. Legal Responses to the Challenge

It is widely argued that the current regulatory approach to such matters is outdated and insufficient, but designing a more appropriate regulatory framework is challenging. It is possible to identify various distinct, though not necessarily mutually exclusive, approaches to addressing this problem.[5]

First, law enforcement might simply be permitted to compel a suspect to assist in decryption by supplying their passwords. This gives rise to practical problems, however, in that the suspect may not yet have been tracked down or may have died (as in the San Bernardino case)

4 Ince, Oxford Dictionary of the Internet, 2nd edn, Oxford 2009.

5 For consideration of existing methods of defeating encryption, see Penney/Gibbs, Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter, 63 McGill Law Journal, 2017, 201.

or may simply refuse to cooperate. This approach also gives rise to questions regarding compatibility with constitutional and human rights. Attempts by the state to compel a suspect to provide incriminatory information will, as a rule, engage the privilege against self-incrimination. It is unclear, however, whether the privilege against self-incrimination as protected by Article 6 ECHR would prevent the authorities from compelling a suspect to provide a password. Although many countries and jurisdictions operate under the assumption that compelled decryption violates the right, this is certainly not the approach in England and Wales.[6] According to sections 49 and 53 of the Regulation of Investigatory Powers Act 2000, it is a criminal offence, punishable by a sentence of imprisonment of up to two years, to fail to disclose when requested the key to any encrypted information. In 2014 a man from Luton, England, was convicted of failing to provide the police with a password for a memory stick seized during a counter terrorism operation (he claimed he could not remember the password but did in fact subsequently remember it – some 11 months later) and jailed for four months.[7]

A second approach is to pass legislation allowing law enforcement to hack into systems to get the data themselves. This approach is also envisaged in the UK investigatory powers legislation and was utilised in the San Bernadino case when the FBI allegedly paid 1.3 million dollars to purchase a hacking tool, which allowed it to access the encrypted content. On the one hand, the approach gives rise to security concerns, on the other, it raises questions about the lawfulness of inciting third parties to produce hacking tools – essentially condoning state sponsored hacking.

Third, legislation could be passed forcing tech companies to retain their ability to decrypt content to ensure that they are able to comply with law enforcement warrants. Examples of this type of solution are to be found in the much-criticised Burr-Feinstein encryption bill in the USA,[8] in the UK Investigatory Powers Act[9] and in French legislation.[10] Such solutions also give rise to various concerns. Tech companies argue that it might result in consumers switching to foreign internet providers – some estimates suggest that the impact of such lost business in the USA would result in losses of in the region of $180 billion. It is unsurprising therefore that the Feinstein-Burr proposal has not received the support of the White House and is not expected by commentators to be enacted.

Aside from the economic consequences of such proposals, if customers switched to foreign internet providers this could actually make it even harder to access content by forcing law enforcement to cooperate with foreign governments to secure access to the information. In those cases, in which the relevant tech companies were based in a foreign jurisdiction, law enforcement would be required to use cumbersome mutual legal assistance treaties – if they exist – to secure assistance.

The main argument against compelled decryption involves security concerns if companies were forced to keep keys to enable decryption. Apple's response, for instance, was to state that it would do its best to 'protect that key, but in a world where all of our data is under constant

6 See eg *R v S* [2008] EWCA Crim 2177; [2009] 1 WLR 1489 where the court held that S had a legal obligation to disclose the encryption key and that compelling S to do so was not unfair. This confidence in compliance with Article 6 ECHR is arguably called into question by the judgment in *Chambaz v Switzerland*, no. 11663/04, 5 April 2012. See also the US case *Boucher II*, 2009 WL 424718 and for discussion Kerr, Compelled Decryption and the Privilege against Self-Incrimination, 97 Texas Law Review 2019, 767.

7 http://www.bbc.com/news/uk-25745989, 15 January 2014.

8 Compliance with Court Orders Act of 2016, discussion draft available at https://www.feinstein.senate.gov/public/_cache/files/5/b/5b990532-cc7f-427f-9942-559e73eb8bfb/6701CF2828167CB85F51D12F7CB69D74.bag16460.pdf [09.09.2019].

9 Investigatory Powers Act 2016, s. 253(5).

10 See Art. 434-15-2 of the criminal code.

threat, it would be relentlessly attacked by hackers and cybercriminals'.[11]

The economic and security concerns of the tech companies and communications operators are clearly well founded and the solutions clearly need to be tailored to take these into account. What, however, is the problem with compelled decryption of third parties? Why should this be considered problematic? Swiss investigation authorities have, after all, long employed the practice of compelling communications operators to assist with unlocking passwords to further drugs prosecutions. This was never viewed as particularly problematic providing that the provisions of the criminal procedure code regulating the search or seizure or interception of the relevant data had been complied with.

This emphasises that the problem here is less the element of compulsion of third parties but rather the legal basis on which the third parties can be compelled to provide assistance in decryption – essentially the existence of a warrant. In this context it is notable, for instance, that under the UK investigatory powers legislation there is no need for reasonable suspicion in order for law enforcement to obtain a warrant for equipment interference if it relates to the detection or prevention of serious crime (defined as a likely sentence of more than three years) providing that it is 'necessary and proportionate'.

Questions arise here not so much as to the legality of such provisions but as to their legitimacy; but how should the legitimacy of such provision be determined?

In modern times, constitutional provisions lend legitimacy to the law. Legislators are not free to enact such laws as they please but are required to comply with the demands of these constitutional provisions. In Europe, the European Convention on Human Rights (ECHR) has played an important role in delineating and safeguarding guaranteeing common standards, which all member states are required to meet. The UK Home Secretary confirmed, as required to do by the Human Rights Act 1998, that in her opinion the draft legislation on the investigatory powers legislation complied with the provisions of the ECHR. Others were not so sure: JUSTICE, for instance, stated that it considered that there were 'serious concerns about the compatibility of these powers with the provisions of the ECHR and the Charter of Fundamental Rights of the European Union.'[12] The legislation was nevertheless subsequently enacted. If such legislation does in fact conform to the requirements of the ECHR, this might reveal a worrying lack of regulation in this sphere. It is useful to consider the scope and limits of the European human rights protections in this context.

IV. The Extent of the Protection in the ECHR

There are limits to a state's power to interfere in the lives of its citizens. In the context of compelled decryption, the principal concern is of course interference in the private lives of individuals. Also of considerable importance, however, are the consequences of the use of such evidence in criminal trials and the impact of this on the fairness of criminal proceedings.

To what extent might the ECHR be said to regulate policing in the context of investigating and preventing crime? What are the consequences of this regulation in the context of compelled decryption or state interference with computer systems? If we turn to the ECHR, we can see that there are several provisions, which might be of relevance, particularly Article 8 ECHR and Article 6 ECHR.

11 See https://www.apple.com/customer-letter/answers [09.09.2019].

12 Justice, Investigatory Powers Bill 2016: Briefing for House of Commons Second Reading, London, UK, March 2016, available at http://2bquk8cdew6192tsu41lay8t.wpengine.netdna-cdn.com/wp-content/uploads/2016/03/JUSTICE-Investigatory-Powers-Bill-2R-Briefing-11-March-2016-FINAL.pdf, last accessed 9.9.2019.

A. Privacy and Article 8 ECHR

Police activity in intercepting, searching or seizing evidence must comply with the privacy guarantee in Article 8 ECHR. The protection of the right to private life under Article 8 ECHR is wide and covers, *inter alia*, both emails[13] and mobile phone communications.[14] Accordingly, if law enforcement authorities proceed to access such data then these actions will interfere with the rights protected by Article 8 ECHR. Interferences with the rights in Article 8 ECHR can, however, in certain circumstances, be justified. Article 8(2) ECHR requires that actions that interfere with protected rights are in accordance with the law, undertaken in pursuance of a legitimate aim and necessary in a democratic society.

The requirement that actions, which interfere with rights protected by Article 8 ECHR are in accordance with the law contains a number of specific aspects. First, the action must have a basis in domestic law. This domestic law must be sufficiently clear and accessible in order to afford individuals the possibility to foresee the circumstances in which it will be applied. In addition, the domestic law must comply with the rule of law and include sufficient protections against arbitrariness. This means that the discretion afforded by the relevant domestic law must not be too wide.[15] These issues are often also considered under the final strand of the justification process as part of the proportionality assessment.[16] The specific formulation of the test is, however, materially irrelevant – at some stage the European Court of Human Rights (ECtHR) will consider the safeguards against arbitrariness when assessing whether the interference with the protected rights under Article 8 ECHR can be justified.

The second leg of the tripartite test – whether the interference pursues a legitimate aim – is seldom at issue before the ECtHR. Article 8(2) ECHR sets out specific legitimate aims that actions that interfere with Article 8 ECHR rights should pursue if they are to be justifiable. These aims include protecting national security, public safety, or preventing disorder or crime. Such aims are easily invoked in relation to the accessing of data or communications by law enforcement authorities.

Finally, the ECtHR considers whether the interference can be considered 'necessary in a democratic society'. The ECtHR first considers whether a 'pressing social need' exists that has motivated the interfering actions. Second, the reasons for the interference must be 'relevant and sufficient'.[17] Finally, the ECtHR conducts a proportionality assessment. This assessment balances the extent of the interference with the reasons for the interference and the pursued legitimate aim. Within the proportionality assessment the ECtHR often also considers the relevant domestic decision making process surrounding the actions that resulted in an interference. Although not mentioned within the text of Article 8 ECHR, the ECtHR has highlighted that affording due process rights to the individual during the domestic decision making process is an important protection against arbitrariness.[18]

Within the ECtHR's vast jurisprudence surrounding Article 8 ECHR, the relevance of 'reasonable suspicion' to justify police activity that interferes with the right in Article 8 ECHR is of particular interest. This has been considered by the ECtHR within the context of 'stop and search' regimes. Here the ECtHR's focus is firmly on the procedural safeguards and domestic decision-making process that act as protections against arbitrary actions by domestic authorities.

13 *Copland v. United Kingdom*, no. 62617/00, 3 April 2007, § 41.

14 *Roman Zakharov v. Russia*, no. 47143/06, 4 December 2015, § 173, and *Liberty and Others v. United Kingdom*, no. 58243/00, 1 July 2008, § 56.

15 *S and Marper v. United Kingdom*, no. 30562/04 and no. 30566/04, 4 December 2008, § 95.

16 *Ibid*, § 99.

17 *Ibid*, §§ 95-101.

18 *McMichael v. United Kingdom*, no. 16424/90, 24 February 1995, § 87

In *Gillan and Quinton* the ECtHR considered whether the 'stop and search' regime within the UK's Terrorism Act 2000 complied with Article 8 ECHR.[19] The domestic legislation allowed senior police officers to afford officers stop and search powers within designated areas for up to 28 days. This allowed officers to stop and search individuals if they believed that it was 'expedient for the prevention of acts of terrorism'. The ECtHR considered that these searches, which were not consented to by individuals, constituted an interference with their right to private life protected by Article 8 ECHR. Following this, the ECtHR assessed whether the interference was 'in accordance with the law'. The ECtHR highlighted a number of deficiencies when considering whether domestic law afforded sufficient protections against arbitrariness and clearly limited the scope of discretion afforded to officers. The procedure surrounding the designation of areas as 'stop and search' areas was firstly unsatisfactory. Although the initial decision required confirmation by the Secretary of State within 48 hours, this had never been withheld.[20] Secondly, the Independent Reviewer had limited powers to only report on application of the regime as opposed to alter or rescind any decisions to set up designated areas. Finally, although the orders were limited in time to 28 days, they were capable of being renewed. Reports showed that these orders were systematically renewed as part of a 'rolling programme'.[21] The domestic system did not include sufficient safeguards to ensure that subsequent interfering powers were not used in an arbitrary manner. The ECtHR also focussed upon the fact that officers could rely on 'expediency' as opposed to 'necessity' or 'reasonableness' when invoking stop and search powers. This gave officers an inappropriately wide discretion that resulted in a clear risk of arbitrary use of the powers. Accordingly, the ECtHR found that domestic law failed to satisfy the requirements imposed by the 'in accordance with the law' test and therefore violated Article 8 ECHR.

The scheme in *Gillan and Quinton* can be compared to that employed in the Netherlands, which was considered by the ECtHR in *Colon*.[22] In this decision, the ECtHR considered that the 'stop and search' regime in the Netherlands included sufficient safeguards to hold that the interferences were 'in accordance with the law'. The domestic regime included strong review mechanisms prior to the decision by public bodies and, also, by criminal courts during subsequent criminal proceedings that arose as a result of a search conducted under the relevant regime. These safeguards were sufficient to protect against the risk of arbitrariness.

This case law emphasises the close relationship between the requirement of existence of reasonable suspicion that a crime has been committed and the prevention of arbitrariness. In the context of encryption, this suggests that the investigation authorities would at least have to have some prima facie evidence that a crime had been committed before they were entitled to act to compel third parties to assist in decryption in order to meet the requirements of Article 8 ECHR. Even assuming, though, that an order to compel a third party to provide assistance in decrypting evidence violated the Article 8 ECHR rights of a suspect, this does not necessarily mean that the use of evidence obtained in violation of Article 8 ECHR will automatically be deemed to compromise the fairness of the trial.

It is noticeable that Article 8 ECHR does not contain an 'exclusionary-type' provision comparable to that of the fourth amendment to the US Constitution. Thus, while the interception and compelled decryption of content is regulated by Article 8 ECHR, a violation of the provision will not necessarily lead to a prohibition on the use of the evidence. Indeed, the ECtHR

19 *Gillan and Quinton v. United Kingdom*, no. 4158/05, 12 January 2010.

20 *Ibid*, § 80.

21 *Ibid*, § 81.

22 *Colon v. Netherlands (dec.)*, no. 49458/06, 15 May 2012.

has proven reluctant – or perhaps more accurately has consistently refused – to find that the use of evidence obtained in violation of Article 8 ECHR automatically violates Article 6 ECHR.[23]

B. Privacy, Fairness and Article 6 ECHR

A good example of the type of reasoning which the ECtHR employs when considering whether a violation of Article 8 ECHR might compromise the fairness of the trial can be found in its judgment in *Bykov*. In this case, it held that in determining whether the proceedings as a whole were fair, 'regard had also be had to whether the rights of the defence were respected'. It noted that it was necessary to examine 'whether the applicant was given the opportunity of challenging the authenticity of the evidence and of opposing its use. In addition, the quality of the evidence must be taken into consideration, including whether the circumstances in which it was obtained cast doubt on its reliability or accuracy. While no problem of fairness necessarily arises where the evidence obtained was unsupported by other material, it may be noted that where the evidence is very strong and there is no risk of its being unreliable, the need for supporting evidence is correspondingly weaker'.[24]

Similarly, in *Khan*, where no statutory system existed at all to regulate the use of covert listening devices, the finding that Article 8 ECHR had been violated was not deemed to impact on the fairness of the subsequent trial. The ECtHR held that the applicant had had 'ample opportunity to challenge both the authenticity and the use of the recording' and that at each level of jurisdiction the domestic courts assessed the effect of admission of the evidence on the fairness of the trial by reference to section 78 of the Police and Criminal Evidence Act. It noted that had the domestic courts been of the view that the admission of the evidence would have given rise to substantive unfairness, they would have had a discretion to exclude it under the relevant legislation.[25]

This type of test places virtually no restraints on police or prosecutorial activity and does little to guard against arbitrariness. Essentially, it represents a requirement of contestability without explaining which standards must be adhered to. Concerns about the fairness of the use of evidence obtained by compelling individuals or third parties to decrypt information are linked to the Article 8 ECHR concerns in that they relate to the potential for arbitrariness in the police or prosecutorial activity. In many, if not the majority of, European countries, this potential for arbitrariness in the context of the prosecution of crime is kept in check by a series of safeguards notably the requirements of reasonable suspicion, subsidiarity and proportionality, which are all subject to judicial supervision and control. There are prohibitions on the use of evidence, which has not been obtained in a manner which meets these requirements.

It is noticeable that the ECHR does not contain any provisions which might be said to afford this type of protection against arbitrariness. The only cases in which the ECtHR has considered a lack of reasonable suspicion in the context of the collection of evidence to impact on the fairness of the trial have involved entrapment or police incitement. In *Kudobin*, for instance, the ECtHR held that reasonable suspicion that the applicant was involved in criminal activity was necessary to rule out arbitrariness. In addition, the fact that the ECtHR has held that the existence of previous convictions is sufficient to give rise to such

23 See eg *Bykov v. Russia* [GC], no. 4378/02, 10 December 2009; *PG and JH v. United Kingdom*, no. 44787/98, ECHR 2001-IX; *Heglas v. Czech Republic*, no. 5935/02, 1 March 2007; *Khan v. United Kingdom*, no. 35394/97, 12 May 2000, Reports 2000-V, and for discussion Jackson/Summers, The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions, Cambridge 2012, 171.

24 *Bykov v. Russia* [GC], no. 4378/02, 10 December 2009, § 90, citing *Khan v. United Kingdom*, no. 35394/97, 12 May 2000, Reports 2000-V, §§ 35 and 37, and *Allan v. United Kingdom*, 31 December 2002, Reports 2002-IX, § 43.

25 *Khan v. United Kingdom*, no. 35394/97, 12 May 2000, Reports 2000-V, § 38.

reasonable suspicion demonstrates the limits of this test.[26]

It is instructive that in the modern age of data collection in which the law enforcement authorities have considerable powers to engage in wide-spread surveillance and interception of communications and bulk collection of data, that the principal European body regulating the fairness of criminal proceedings has little to contribute to developing an appropriate regulatory framework. This is once again evidence of the trial-centric approach to the regulation of criminal trials; an approach which relies on an artificial split between the investigative and determinative phases of the proceedings and which relies on the opportunity to challenge the manner in which the evidence was collected as sufficient to remedy any potential infringements in the collection of evidence.

V. Conclusion

An appropriate regulatory structure governing search and seizure and compulsion to assist in decryption would involve consideration of the need to prevent arbitrary or discriminatory policing and investigation. An appropriate regulatory framework would involve a clear distinction being made between prevention and prosecution of crime. In those cases, in which the police investigations are based on suspicion about a particular suspect, the guarantee against arbitrariness is provided by the requirements of reasonable suspicion and proportionality. In relation to the prevention of crime and suspicionless searches, arbitrariness would be prevented by generality and proportionality – the guarantee here is essentially the random nature of such searches.[27] This focuses attention both on the weaknesses of the current European human rights framework in the context of technological development and on the importance of thinking more about the connection between fairness and a lack of arbitrariness in the investigation of crime. Can trials constructed on the basis of evidence collected by way of arbitrary or discriminatory policing techniques be said to be fair? If not, why not? And what type of remedies ought to be employed in order to uphold this understanding of fairness?

26 *Khudobin v. Russia*, no. 59696/00, 26 October 2006, § 134.

27 Friedman/Benin Stein, Redefining what's reasonable: The protections for policing, 84 George Washington Law Review, 2016, 281.