Report of findings by the technical-substantive task force on encryption

Definitively adopted on: 25 March 2022

Introduction

The following is a report from an ad hoc task force whose members included Mr Jacobs and Mr Van Eeten of the Cyber Security Council (CSR), and which met online a number of times in the three-month period of November 2021 through January 2022. Other participants of this task force included:

- Two operational digital specialists from the High-tech Crime Team of the National Police;
- A representative from the AIVD with a technical/policy background;
- A senior adviser from the Ministry of Justice and Security's Platform for Interception, Decryption & Signal analysis (PIDS);
- A senior policy adviser from the Directorate of Digital Economy/Director-General for Enterprise and Innovation at the Ministry of Economic Affairs and Climate Policy;
- A Strategy and Policy Adviser from the KPN CISO Office.

The task force was supervised by a senior adviser from the secretariat's office of the CSR.

The issue/task which the task force was convened to address is as follows:

What realistic alternatives exist for gaining lawful access to end-to-end encrypted communication, other than weakening encryption?

The purpose of the task force was therefore emphatically *not* to explore possibilities for cracking encryption, but to investigate alternatives to doing so. During a number of internal expert sessions, the task force examined the full breadth of the issue and arrived at two key topics: (1) **hacking**, carried out by police and intelligence services, and (2) **requests for operational logs**, i.e., the data collected by businesses for operational management purposes. Following a brief introduction, this report will address these two topics in greater detail before arriving at a number of recommendations.

When in the following document, mention is made of interception (tapping) of telephone services and other forms of communication, the assumption is always that this is carried out exclusively by the bodies authorised to do so (primarily the police and intelligence/security services) within the relevant existing legal frameworks, with the proper permission and under various forms of supervision. The same applies to the deployment of so-called hacking powers. A highly diverse range of activities are conducted under this power. These activities vary from direct or forensic duplication of a USB stick or hard drive to carrying out complex hacking operations aimed at large networks. When the act of ‘hacking’ is discussed, this inevitably refers to gaining remote access to computers. That interpretation is adhered to here as well.

In recent decades, tapping has been fully codified at the international level, in the technical, organisational and legal sense. This standardisation (public and otherwise) of interfaces and architecture for interception offers many advantages: on the one hand, providing legal certainty for citizens and on the other, ensuring professional clarity and feasibility for clients and implementing parties. The commercially available telecom infrastructure includes this standardised tap functionality.

With the end-to-end (E2E) encryption of modern, popular over-the-top (OTT) messaging services (such as WhatsApp, Signal and Telegram), this accessibility and ready oversight has been permanently eliminated. Because a clear structure such as the one which served for tapping telephones does not exist with regard to OTT services (and is not expected to be introduced in the short to medium term), it is crucial that we obtain a picture of the spectrum of alternatives that are readily available. This memo focuses on the technical aspects and makes no mention of legal alternatives such as expanding the possibilities for online infiltration. This memo was drafted in a short period of time based on research with an extremely limited scope; it does not presume to be comprehensive.

It is also worth noting that phone tapping is also under pressure from sources besides the availability of these OTT services. There is no international clarity yet with regard to the 5G infrastructure currently being rolled out. The encryption of signal information in the 5G network means that a foreign 5G smartphone cannot, in principle, be tapped in the Netherlands. This problem also exists the other way round. The decryption of the signal data (and therefore the tap) can take place only in the country of origin. In order to make domestic tapping of international smartphones possible, the terms of the (hundreds) of roaming agreements between telecom providers must allow for this encryption to be switched off. On the one hand, providers are under pressure from their clients (and GDPR) to make use of encryption, while on the other hand, they face pressure from judicial authorities (in Europe) *not* to deploy encryption in order to make international phone taps possible. This debate is ongoing, with the Netherlands playing an active role within Europe. That discussion itself will not be further addressed in this report.

1. Hacking

Since the Intelligence and Security Services Act (WiV) entered into force in 2002, intelligence & security services have had legal grounds for accessing computers belonging to targets, whether directly or indirectly. The 2019 Computer Crime Act III has granted the police similar powers to remotely access computers. Where intelligence & security services are concerned, hacking has become a standard part of the performance of their duties. For the police, however, hacking remains less thoroughly embedded and well-defined (see the 2020 report on supervision concerning the statutory power of the police to carry out hacking operations and the yet-to-be-published report from the Research and Documentation Centre). The police are dealing with greater limitations in their ability to carry out hacks, particularly with regard to the tools and vulnerabilities they are permitted to deploy.

To a certain extent, hacking may involve the use of tools (or scripts) that are either purchased or built by the user. The market for these tools is controversial, as evidenced by the discussion surrounding the Israeli firm NSO, which has now been banned in the U.S. While such tools could potentially make hacking easier, they have the disadvantage that – because of the uniform method they employ – they can be recognised by targets. In addition, the long term-effectiveness of these tools is uncertain because the vulnerabilities they currently exploit may become unusable at a future point, typically due to a patch.

Hacking is by and large a situation-specific and manual undertaking. As a law enforcement technique, it has not yet been standardised – nationally or internationally – in either the technical, organisational or legal sense. Both administrative and operational costs are high and capacity is limited, forming an impediment to its application. Neither is it scalable: doubling your hacking output requires doubling the number of hackers.

Still, hacking has yielded impressive results in recent years, such as the dismantling of various secure communication networks used by criminals. Particularly for this kind of major case, with a longer duration, hacking has proven to be a suitable approach. Yet here, too, there is no way to be certain of the output in advance.

Hacks can be aimed at hosting or other infrastructure and against the suspects or targets who are active there. Hacking smartphones has been adopted more slowly because the legal grounds necessary to do so were less readily apparent. Improvement is conceivable in this area via new legal and technical regulations that will provide police and intelligence & security services with a better starting position in dealing with telecom providers, so that they may obtain direct access to the message flows to and from a specific smartphone. This method (necessarily) preserves the integrity of end-to-end encryption while offering a better approach to accessing a specific smartphone via a hacking operation.

2. Operational logs

Because OTT services are encrypted end-to-end, the companies that provide these services do not themselves have access to the content of the communication. That being said, they do store all kinds of operational data (logs) relating to that communication for purposes such as providing the service and detecting fraud, as well as for profiling and marketing. This data concerns the identities of the parties involved, the contacts, times, locations, dates, duration, size and nature of the messages, and so on. These businesses are able to perform checks of the smartphones in their own apps, in which they can also offer the option of creating a (potentially encrypted) backup of the message traffic. Generally speaking, the exact nature of what they monitor and retain is unknown.

The Dutch police and intelligence & security services request data from the (often American) providers of OTT services with some regularity. In such instances, the difference between the legal systems of the Netherlands/Europe and that of the U.S. come into play, as do the differences in how they define and interpret certain concepts. In the Netherlands, a distinction is generally made between identifying data and non-identifying data, in keeping with the GDPR. In the United States, the distinction between content and meta data is of greater significance. These distinctions do not align with one another. In the Netherlands, for instance, location data is considered meta data, whereas it is seen as content in the U.S. In practice, account information (that has been registered when the account is created) may be requested directly from the company itself and is typically supplied in relatively short order (a number of weeks). Other information, including user data, must be requested from the U.S. Department of Justice. That procedure is more time-consuming (typically taking months) and usually fails to yield all the information. The companies involved often delay complying with requests, claiming that they do not know where the requested data is stored. The majority of Dutch requests therefore involve account information.

Investigators with the police and intelligence & security services are often motivated to close individual cases without concern for a strategic long-term perspective. They are accustomed to pursuing various avenues and switch easily from one approach to another when the results in question disappoint. Consequently, delayed provision of or failure to provide operational logs has never become a fundamental issue and legal proceedings have never been initiated to compel the handover of data, or to compel faster or more extensive results. To our knowledge, neither has anyone ever sought to address the relevant companies under Dutch law by means of their branch offices in the Netherlands. There is room for improvement in this regard. The legal basis for domestic and international data requests could stand to be strengthened as well. In addition, public-private partnerships aimed at combating fraud offer an opportunity for a more effective approach, including assistance for victims.

3. Recommendations

1. Rather than attempting to compensate for the reduced output from traditional well-organised phone taps by means of a single measure, take a wider view of the matter by considering a spectrum of possible alternative approaches.

1. Embed and streamline hacking as an investigative tool used by police, in keeping with the upcoming WODC report, while also recognising that there are significant impediments to the use of hacking, that it is difficult to scale up, is situation-specific, is suitable primarily for major cases and is not guaranteed to yield the desired output.

2. With regard to tapping 5G connections, implementation at the European level calls for the same transparency, uniformity and legal certainty which are now prevalent in the telecom industry.

3. Investigate the possibility of transparent legal regulations for enhanced access to telecom providers for the purpose of securing a better starting position for being able to hack specific smartphones.

4. Compel providers of online services to cooperate more closely and to provide operational data (logs). This can be achieved in the near term via case law and in the longer term via national and international legislation.

5. Approach these requests for information from a more Dutch/European perspective in order to avoid issues of interpretation under American law. Possible starting points in this regard are: the Dutch/European branch offices of the relevant companies, as well as the European perspective on data which holds that authority/ownership lies with the data subjects rather than the processing organisations.

6. Establish more intensive public-private partnerships with the fraud departments of companies that provide services in the information society. This cooperation should emphasise the duty of care owed to society by large ICT companies.