Remote Search by Justice Authorities

Steven Rekke, Menno van Wieringen, Aram Verstegen
??, ??, 4092368

1 Introduction

In the Netherlands there has recently been some commotion around the use of *Remote Forensic Software* (RFS) to obtain information from targeted computers.

A national political party asked the Dutch minister of Security and Justice for elucidation about the lawfulness of the use of remote surveillance software by the authorities within the Netherlands. ['66]

The Dutch state counsel (OM) replied to this question by answering that the use of RFS tools is covered by article 126i and 126m of the code of Strafvordering (Criminal law), and also stated that rules for this are elaborated upon further in an Order of Council. Finally, they stated that the RFS software is only used as a key logger or to record audio via a microphone; using the webcam to record video is not currently implemented. [Web]

As we understand the matter, this is somewhat of a grey area in the law, falling somewhere between the areas of legislation in criminal, data retention and privacy laws. We are tasked with advising the courts on how existing legislation surrounding RFS tools in use by justice authorities should be interpreted, and whether new legislation is deemed necessary. We have chosen to look at neighbour states dealing with the same issues for legal precedents, and will reference these in the answers to the presented questions where relevant.

2 Questions presented

1. Does local legislation allow for Remote Forensic Software? (How should existing legislation be interpreted?)
2. Does the EU need new legislation to regulate the use of Remote Forensic Software?
   (a) What is the added value of such legislation?
   (b) What are required safeguards?

3 Short answer

1. Yes, it does in principle. The Dutch state counsel (OM) has informally stated that there is legal ground for the use of RFS tools in response to the questions posed to the minister of Security and Justice in parliament, and stipulates that the use of such tools may only occur following directions of the public prosecutor. [Web] This is true in the sense that the law grants Special Powers of Investigation to some justice authorities, among which the power to "record confidential communications by means of a technical aid". [dNd]

   The German Federal Court has determined that RFS is sufficiently different from other investigation techniques to require explicit legislation to create a new police power. The German Constitutional Court (FCC) has determined that a new absolute constitutional right applies which limits the application of RFS, but RFS itself is not found unconstitutional.

   In the United Kingdom, the use of RFS is mandated by the Regulation of Investigatory Powers Act, which allows remote wiretapping, the local placement of bugging devices, and other, less well-defined forms of intrusive surveillance. [Arcb]

2. Yes, it does. While Dutch criminal law has provisions for the use of 'technical aids' in prosecution, where it mentions the use of electronic devices to intercept traffic it appears to mean a 'network tap', but makes no specific statements for or against the use of active, remote forensics software.

   In the United Kingdom, the relevant provisions in the Regulation of Investigatory Powers Act makes general exemptions for the use of technical surveillance tools, but again does not make explicit their reach and technical paradigm (active or passive). There exist general provisions allowing the aggregation and processing of personal data by law enforcement agencies in the UK Data Protection Act, but they also make no explicit distinction in active or passive gathering of information.

   The German example shows that a mere advisory statement by the council of the European union does not provide enough legal foundation to implement the use of RFS.

4 Statement of facts

In a statement on measures against cybercrime, the Council of the European Union (EU) advised member states to perform clandestine remote searches of suspects' computers as a means to combat cybercrime. These remote searches are executed using so-called *Remote Forensic Software* (RFS) tools.

4.1 the Netherlands

When we look into the specific text of article 126i [dNb], it is stated that the justice department can order an investigating officer to intercept communication using a tech-

nical tool. It is also stated that a closed off area or a house may be entered without the approval of its owner. It seems that the article refers to physical areas and not to digital computer areas. It all depends on the interpretation of 'closed off area'.

In article 126m [dNc], it is stated that the justice department can order an investigating officer to intercept communication using a technical tool that is not meant for the public domain, and which is run by a provider of communication services on behalf of the justice authorities. This allows placement of telephone taps, and in modern times, network taps at land-line or internet exchange level. Allowing the placement of an active software tap (RFS) on a computer that uses the services of the communication provider is not well-defined in the law.

4.2 Germany

In Germany, the concept of RFS tools was officially introduced 2006, when German Prosecution authorities applied for a search warrant to remotely search a suspect's computer (Ref. 1). This application was rejected, but triggered a public debate about the legality of remotely searching a suspect's computer (Ref. 2). In its decision to deny the application for a search warrant, the Federal Court of Justice avoided to discuss the legal issues that surround the use of an RFS tool. The court however, did indicate that remote searches are different from existing investigation techniques and require explicit legislation to create a new police power. Neither the laws regulating mail intercepts, nor those regulating telephone surveillance were deemed appropriate. So to enable the use of RFS, the German government needed legislation to meet these requirements. As most policing functions are regulated on state level, it was now up to individual states to adjust their legislation to enable the use of RFS. In December 2006, the state of Nordrhein-Westfalen was the first state to enable the use of RFS by their constitutional protection agency through an amendment of its law for the protection of the constitution (Verfassungsschutzgesetz). This paragraph (Article 5 II Par. 11, VSG NRW) permitted the secret observation, investigation and clandestine interception of communication via the Internet and access to its IT systems. In a response to this amendment, a constitutional complaint was filed with the German Federal Constitutional Court (FCC) to challenge its constitutionality. On February 27th of 2008, the FCC ruled that the amendment to the Verfassungsschutzgesetz was in fact unconstitutional and thus unlawful. The FCC did not, however, declare all use of RFS unconstitutional. Instead, the FCC recognized a new constitutional right: the confidentiality and integrity of information technology systems. As this constitutional right can only be limited in the interest of other constitutional rights, the FCC through their judgment have given limit and scope to the use of RFC in Germany.

4.3 United Kingdom

A spokesman for the Association of Chief Police Officers, officiously and anonymously commented that surveillance using RFS was regulated under the Regulation of Investigatory Powers Act, when prompted by the Independent. [Ind] Looking at the law, we

find it does indeed provide justice authorities with a legal basis for what it terms 'intrusive surveillance' in the interest of national security. [Arcb] Interestingly, it goes on to define that surveillance is intrusive if it "it is carried out by means only of a surveillance device designed or adapted principally for the purpose of providing information about the location of a vehicle; or", "it is surveillance consisting in any such interception of a communication as falls within section 48(4)" in section 26,article 4.

UK law also sets a legal standard for the use of collected personal data in the Data Protection Act [Arca], and makes specific exemptions for law enforcement and, in particular, agencies upholding national security. Similar to Dutch regulation, it allows law enforcement to retrieve and process electronic data from telecommunications networks, but does not make explicit recommendations for or against active wiretaps like RFS tools can provide. Crucially, the subject of investigation need not be informed of information being collected if it is done under such an exemption.

5 Discussion

5.1 the Netherlands

The Order of Council describing technical tools, "Besluit Technische Hulpmiddelen Strafvordering" which looses translates to "Decision on technical aids in criminal procedure" [dNa] describes what a technical tool should be, but remains vague other than a reference to another article (namely 26ee, part a - which states that the technical tools as referenced in a few articles are technical tools). In this article the technical tools are allowed to gain information, but still there are more points to consider.

"By or on behalf of the force manager, a place for the storage of technical aids and ensure that the nominated site is secure and accessible only by or under the supervision of authorized personnel."

The question here is: how would one install and hide the RFS on a computer, as the machine may be or become accessible to experts putting the RFS to use for their own (malicious) purposes. This means that the security of a digital product needs to be done on a physical way. That is storing it on a media device looked up in a secure location.

"The removal of the technical device made by a duly appointed by or on behalf of the force manager and expert in the field investigating officer."

Another question that arises is how could one make sure that the distributed RFS is removed when it is not in use anymore, because it is possible that the computer containing the RFS is disconnected from the internet, preventing remote removal of the software.

5.2 Germany

When the German Court had to decide on whether or not to provide the search warrant requesting the use of RFS, they had to investigate whether RFS could be subsumed under existing legal concepts. Two possible matches in existing legislation were identified: the

search of premises, and interceptions of telecommunication. Both these measures are regulated by the German Criminal Procedural Code (Strafprozessordnung – StPO).

Under these regulations, search of a person's premises and belongings is allowed if it is believed to lead to the discovery of evidence. Case law points out that this includes the search and confiscation of data stored on data storage devices (Ref. 3). This would seem to suffice for RFS purposes, as it is irrelevant to the rule whether this search occurs remotely or in person. There is, however, a substantial difference because search using RFS tools occurs without the knowledge of the suspect. Several rules in StPO (article 105, 106, 107) ensure that the subject of the search is informed about the reason for the search and they can verify that the search is legitimate. This led the court to decide that the search of premises is an insufficient match for RFS.

The second possible investigative technique to use as an analogy is the interception of telecommunications, which is regulated under article 100a StPO. This article allows for monitoring and recording of communications. Under specific circumstances this is allowed even without the subject being aware. An essential part of these regulations is that the target of the interception is a data flow between suspect and a third party. The purely technical means of transmitting data from the RFS to the investigating party is not the thing that is intercepted, and is not the subject of the investigation. RFS can therefore not be regulated under interception of telecommunications legislation.

When both these analogies proved insufficient, the court decided that new legislation was required to enable RFS tools to be used. This new legislation first came in the form of an amendment of article 5 of the Verfassungsschutzgesetz of Nordrhein-Westfalen.

The constitutional court then determined that this amendment was unconstitutional, because it is in violation of a new constitutional right: the confidentiality and integrity of IT systems. This new right was derived from a basic constitutional right in the German constitution, namely the protection of human dignity. This new human right limits the use of RFS tools, as their use now needs to be in accordance with this human right. The new human right can only be limited if the measure restricting the right is proportionate, i.e. if sufficient evidence exists that other fundamental rights are protected by this measure. This means that the use of RFS comes with several important requirements. It can only be used to prevent serious crimes, it can only be permitted by a judge on a case-by-case basis and it cannot violate the core area of the private conduct of life.

Because it is difficult to differentiate between data that does, or does not, affect the core area of private conduct of life the court states that adequate procedures need to be in place for the examination stage of the data. If core data is detected, it needs to be deleted immediately and the use of such data is prohibited. The selection process needs to be done by an investigating judge, a state attorney, or a judicial officer. The German judicial system is not thought to have the manpower to actually implement these procedures, crippling the user of RFS even further.

5.3 United Kingdom

UK law lacks case law where the lawfulness of the use of RFS tools has been contested.

The Regulation of Investigatory Powers Act is different to the Dutch book of Strafvordering, in that it specifically deals with investigatory powers regarding the interception of communications data. As it was specifically introduced to deal with modern surveillance and interception issues, it specifies legal requirements for the use of technical surveillance tools and hints at their lawful applications. [Arcb]

It makes the distinction between various levels of surveillance, ranging from the interception of communications (wiretapping) to what is termed *intrusive surveillance*, namely the placing of eavesdropping equipment. Crucially, it does not make the distinction between physical hardware bugs and ethereal software solutions. One could argue the law leaves this area open to interpretation, but the latter implementation of such a tool has much farther-reaching consequences in terms of data privacy. A rogue actor in law enforcement could employ these tools unlawfully, and there might be little evidence in terms of a 'paper trail' to convict such individuals for their abuse.

The UK Data Protection Act of 1998 defines its 'data protection principles' in Schedule 1, such as the requirement that data is obtained for a specific purpose and may not be further processed, stored excessively long or transported to overseas jurisdictions. [Arca] The law makes various exemptions to its regulations on obtaining personal data for agencies operating on behalf of justice authorities for the purposes of national security, crime and taxation. It exempts national security services from all the data protection principles if deemed necessary, and exempts law enforcement agencies from the general obligation to not retrieve personal data. Schedule 3 of the law makes more specific requirements for the exemption from the requirement to not process *sensitive* personal data.

If an officer of the law were to breach the terms of these exemptions, there is quite clearly a suitable legal framework to pursue a conviction.

6 Conclusion

Following from the discussion presented above, we come to the conclusion that the local legislation does allow for RFS tools to be used, in principle. There are, however, a great number of safeguards in place to restrict and guide the use of RFS in Germany. The question arises whether RFS might still be used efficiently under these restrictions.

The German example shows that the use of Remote Forensic Software comes with several legal issues and that their use may be in violation of local legislation and even the constitution of EU member states. Furthermore, it shows that if the European Union wishes to promote the use of RFS tools, it should provide legal foothold for the member states to implement these measures.

The local laws all lack a clear provision for the use of *software* tools; they simply provide a framework for various levels of surveillance and allow the use of otherwise unspecified technical tools to accomplish it. We find the difference between active and passive approaches too big to be disregarded by the law, and feel it should be made explicit.

The problem we see in the application of RFS tools is that there is little accountability in the 'placement', or rather employment of a non-physical (software) tool. Taking into

account the possibility that the RFS tool be delivered to targeted individuals via some *e-government* website - for example, one to submit tax reports - has the secondary effect that citizens might become cynical or distrustful towards their own government's intelligence operations.

The industry surrounding computer surveillance is rapidly growing, and remains suspiciously shy of press or citizen involvement, or even observance. A final issue of concern is that such software vendors export their tools to repressive regimes outside of the EU, something that in some cases might be considered aiding an enemy regime, or in some cases even assisting in a human rights violation. [Gua]

Especially given the mobile nature of present-day EU citizens and their computers, the implementation calls for EU wide regulations. An RFS tool that is used on the PC of a suspect who crosses a national border would result in several jurisdictional issues. The added value of EU legislation could be that such jurisdictional issues might be resolved before they arise.

References

['66] Democraten '66. Gebruikt nederlandse overheid ook spyware? `http://www.d66.nl/europa/nieuws/20111011/gebruikt_nederlandse_overheid_ook?ctx=vghpm7u9vdea`.

[Arca] The UK National Archives. Data protection act 1998. `http://www.legislation.gov.uk/ukpga/1998/29/contents`.

[Arcb] The UK National Archives. Regulation of investigatory powers act 2000. `http://www.legislation.gov.uk/ukpga/2000/23/contents`.

[dNa] Staat der Nederlanden. Besluit technische hulpmiddelen strafvordering. `http://www.st-ab.nl/wettennr03/0273-024_Besluit_technische_hulpmiddelen_strafvordering.htm`.

[dNb] Staat der Nederlanden. Wetboek van strafvordering, artikel 126i. `http://wetten.overheid.nl/BWBR0001903/EersteBoek/TitelIVA/Derdeafdeling/Artikel126i/geldigheidsdatum_13-11-2011`.

[dNc] Staat der Nederlanden. Wetboek van strafvordering, artikel 126m. `http://wetten.overheid.nl/BWBR0001903/EersteBoek/TitelIVA/Zevendeafdeling/Artikel126m/geldigheidsdatum_13-11-2011`.

[dNd] Staat der Nederlanden. Wijzigingswet wetboek van strafvordering (bijzondere opsporingsbevoegdheden). `http://wetten.overheid.nl/BWBR0010478/geldigheidsdatum_13-11-2011`.

[Gua] The Guardian. Governments turn to hacking techniques for surveillance of citizens. `http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance`.

[Ind] The Independent. New powers for police to hack your pc. http://www.independent.co.uk/news/uk/home-news/new-powers-for-police-to-hack-your-pc-1225802.html.

[Web] Webwereld. Om: gebruik spyware door politie is legaal. http://webwereld.nl/nieuws/108262/om--gebruik-spyware-door-politie-is-legaal.html.