Report on the Criminal Justice Process against "AN.ON - Anonymity.Online"

Helmut Bäumler, Hannes Federrath, Claudia Golembiewski
(Translated from the original German text by Derek Daniel)
September 2003

1 Contact by the Criminal Justice Authorities

In a fax received on June 23, 2003, the Hessian state criminal office (Landeskriminalamt, LKA) requested help from the Technical University, Dresden in determining a user's IP address for a case regarding possession of child pornography magazines. The user had clearly used the anonymization service in the past. As in all previous cases, the Hessian state criminal office (LKA) was notified in writing by the Independent State Center for Data Privacy (Unabhängigen Landeszentrum für Datenschutz, ULD) that no user data is collected or retained and therefore no further information could be given.

Before the ULD's written notification was received by the LKA, an official contacted project staff at the TU-Dresden and inquired whether surveillance and thus identification of a user would be possible in the future and whether this could be done quickly.

The goal of the surveillance would be the tracking of accesses to a particular URL, which would lead to determining from which IP address the access to the URL took place. Project staff confirmed that this type of surveillance would be technically possible, but would require a judicial order. The police official apparently had no problem immediately obtaining such a judicial order and announced that the order would soon be issued. The official was then referred to the ULD for any further attempts at contact.

As a result of this inquiry, the project partners discussed internally how and on what legal basis such a tracking of individual cases might be realized. It was decided that

cooperation with the criminal justice authorities would be given within the realm of technical feasibility and legal necessity in individual cases that met legal requirements, in other words cases with a judicial order in accordance with paragraphs 100 a and b of the criminal process regulation (Strafprozessordnung, StPO). Thus, a function for such tracking was programmed into the current version of the mix server. (See section 3 below for the technical realization of the tracking function.)

On June 30, 2003, an official from the Federal Bureau of Criminal Investigation (Bundeskriminalamt, BKA) contacted the ULD by telephone. Evidently, the BKA had taken over the investigation. The official explained that accesses to a specific internet forum were to be kept under surveillance and asked which legal basis would be necessary for such a warrant to be issued and to whom that warrant should be issued. The ULD staff informed him that a warrant based on paragraphs 100 a and b of the StPO, in other words in accordance with telecommunications surveillance regulations, would be necessary in order for accesses to a specific URL to be recorded. The official gave the impression that such a court order could be obtained on short notice. Four days passed before the BKA faxed a court order from a court in Frankfurt Main to the ULD.

2 Court Order Issued to the ULD

The official from the BKA, who was interested in accesses to a single internet forum, was explicitly told that a court order would need to be based on paragraphs 100 a and b of the StPO. In spite of this, the court order that was issued was surprisingly based on paragraphs 100 g and h of the StPO. While the regulations in paragraphs 100 a and b allow for the future surveillance of telecommunications, paragraphs 100 g and h can only be used to obtain telecommunications connection data (including IP addresses) from connections which have already occurred.

This type of court order only applies to data that is collected and saved by the service provider under current regulations, insofar as they already exist. In accordance with the telecommunication services privacy law (Teledienstedatenschutzgesetzes, TDDSG),

however, the anonymization service does not collect or save such data which could be used to track users, for example IP addresses. Therefore, the court order according to paragraphs 100 g and h of the StPO would not have produced any usable results.

According to the legal reasoning behind paragraphs 100 g and h of the StPO, the saving of connection data is not required for the purpose of crime prevention as it is by paragraph 100 a (see BTDrucksache 14/7008, page 7). Therefore, requiring the anonymization service to track connections cannot be ordered on the basis of paragraphs 100 g and h of the StPO. The material and formal requirements for surveillance according to paragraph 100 a of the StPO (only used for specific crimes in a cataloged list) are significantly higher than those for obtaining information according to paragraphs 100 g and h of the StPO ("crime of a significant nature"). Although paragraph 100 g, section 1, sentence 3 of the StPO states that information collection over future telecommunications connections can be ordered, this regulation says nothing about the legal basis for such information collection.

Based on conversations with police officials, it was believed that in the current case, data that was not normally collected by the anonymization service was to be collected. Thus, only a court order according to paragraphs 100 a and b of the StPO could be used to this end.

The order to collect and retain data could only be given be fulfilling all the requirements of paragraph 100 a of the StPO. There must be the suspicion of one of the specific crimes in the cataloged list of crimes. A court order based on paragraph 100 a of the StPO was clearly not requested by the police or district attorney's office, possibly because the requirements for that type of court order were not fulfilled. The question of legal basis for the actions of the police in this case is not simply an abstract matter of legal formality. Rather, the requirements to be fulfilled for the issuance of a court order based on paragraphs 100 g and h of the StPO ("crime of a significant nature") are

significantly higher than those needed for a court order based on paragraphs 100 a and b of the StPO (specific crimes listed in a cataloged list).

Because of the clearly incorrect legal standing of the court order issued to the ULD, the ULD immediately filed a complaint with the state court in Frankfurt am Main. In the complaint filed by the ULD and in an extended statement, the ULD specified the dominant legal literature, as well as the judicial statement behind paragraphs 100 g and h of the StPO as the basis for the complaint. At the same time, the carrying out of the court order was appealed. Because the complaint filed could not suspend the court order directly, it was necessary to carry out the court order during the process of appeal.

Incidentally, the IP addresses that the BKA officials requested to be put under surveillance was not listed in the court order, rather only in the unofficial cover letter attached to the court order.

3 Carrying Out the Court Order

According to the court order, "the Independent State Center for Data Privacy (ULD) in Schleswig-Holstein is ordered, based on paragraphs 100 g and h of the StPO, paragraph 3, number 16 TKG, to release information on the telecommunications of the remote IP address 141.76.1.122 registered as 'JAP', until 2.10.2003."

The IP address 141.76.1.122 is one of the IP addresses under which JAP users surf the internet anonymously.

To follow the court order as it was written would have required releasing information from all IP addresses of all JAP users. Aside from the fact that this is technically not possible due to the immense amount of data involved, this would have also resulted in the complete surveillance of all users, which was also not the intention of the criminal police. Furthermore, such a complete surveillance is illegal and unjustifiable according to the regulations in the telecommunication services privacy law (TDDSG).

The project partners came to the conclusion that the court order could only be viewed together with the attached cover letter from the BKA, and could only be carried out within its frame.

The IP address named in the BKA cover letter was entered in the final mix server in the cascade so that if the IP address, which was part of a URL, was accessed, the requesting IP address, date, and time could be logged. No other websites and no other users of the AN.ON service were affected by the protocolling function.

The JAP system is still under construction and testing. Currently, some cascades are being operated which are entirely under the control of the project partners. Particularly, the default test cascade used by most users, Dresden-Dresden, is exclusively run by the TU Dresden.

Since the JAP software being developed is open-source, the source code of the current mix software has always been and remains public for any person to examine. Thus the surveillance function also became public known. Through the high popularity and distribution of the software, speculation soon began in the news and discussion forums, whether the service providers were observing the AN.ON users. The "crime detection" function implemented in the mix software was discovered by the open-source community. At about the same time, a required update of the client software was released. Many users were irritated by this because they saw a connection between the new function implementation and the required update. The required update had nothing to do with the protocolling function, however.

Since it is generally not allowed to release information about ongoing investigations, the project partners did not go public with the court order. This was a mistake because on one hand, there was no indication on the website that the crime prevention function had been activated, while at the same time, this could be determined by looking at the changes in the source code. This lead to confusion and doubt among informed users.

The project partners were forced to decide between the legal requirement of not disclosing information about ongoing investigations, and their own goal of transparence toward users. They were in a situation for which they were inadequately prepared. The project under no circumstances wanted to lose the trust of the anonymity service users, so once the crime prevention function became known in internet forums, all further developments of the case were immediately made public in press releases that did not cover specifics of the case. (See press releases from the ULD from August 19, 2003, August 27, 2003, and September 2, 2003.)

4 Results of the Conflict

Due to the complaint filed by the project partners, the Frankfurt am Main state court repealed the district court's order on July 11, 2003. However, this repeal first arrived at the ULD on August 26, 2003. According to the attached note, the repeal from the state court was not sent sooner due to a "technical mistake".

The project partners immediately deactivated the crime prevention protocolling function upon being informed of the court order repeal. Up to this point, only one single access to the IP address in question was logged. Because this access was in the time frame between July 11, 2003 and August 26, 2003 and therefore, from the point of view of the project partners extremely questionable whether it could at all be justified to use, the data was not given to the criminal police. Much more, they took the position that the use of this data that was under the protection of the project partners could certainly only ever be used after a final decision from the state court. This was reported in a press release on August 27, 2003.

In spite of the repeal decision by the state court, the BKA was given a search-and-seizure order by the Frankfurt am Main district court. Officials from the BKA and Sachsen LKA came to the private home of the institute's director for system architecture in computer science on Saturday, August 30, 2003 and demanded the logged data. To prevent further damage (through searching of institute rooms and confiscation of institute computers) to

the TU Dresden and the project partners, the logged data was relinquished under protest to the officials. An official complaint was filed against this court order as well. According to the project partners' position, the search-and-seizure order issued by the district court was an illegal circumvention of the state court's decision. The BKA should not have been allowed to dodge the preliminary decision by the state court in favor of the AN.ON position by obtaining a general search-and-seizure order according to paragraphs 103 and 105 of the StPO. A judicial examination of the actions of the BKA officials is absolutely required.

With a new decision on September 15, 2003, the Frankfurt am Main state court reversed the district court's order to provide information to the criminal police. The court stated, "The regulations under paragraphs 100 g and h of the StPO only apply to cases where data is collected and saved already, which does not occur in this case." The court was referring to the appropriate conduct of the complainant, the ULD. After the preliminary partial success in the suspension of the order, the ULD now also had won the complaint case. The second complaint, the one against the district court's search-and-seizure order on August 30, 2003, remains open. The state court in Frankfurt am Main has not yet reached a decision.

5 Lessons for the Future

The project partners were, at first, not aware of the tension situation between the two needs of strong anonymity and crime prevention. They had planned the AN.ON project in two phases. Phase one would test the technical feasibility of the project and phase two would resolve the technical and legal questions of crime prevention. Through the actions of the BKA, the project partners were forced to take positions on such questions immediately. Basically, they decided on a policy that protects the strong anonymity of AN.ON users for the future, but is also in accordance with legal regulations. A precautionary mass protocolling was rejected and also will not be carried out in the future. That would clearly break telecommunications privacy laws. Strictly following the letter of the law also means following judicial orders, however.

If a judicial order according to paragraph 100 a of the StPO is issued, then it also applies to AN.ON. According to these regulations, surveillance and recording of telecommunications can be ordered when it is suspected that someone has committed or plans to commit one of the specific crimes in the cataloged list of crimes. A further requirement is that the investigation of a person or discovery of that person's whereabouts is not possible or extremely difficult to obtain through other methods. The order may only be carried out against the suspect or persons who, based on specific facts, it is believed are passing messages to or from the suspect or allowing the suspect to use their communications connections. Such an order is limited to three months, but can be extended. The use of any data acquired is limited by further legal restrictions.

As part of the ongoing work on AN.ON, the project partners have decided to make a mass surveillance of all users technically impossible. The surveillance of individual cases should be possible in a form that no other users could ever fall under that surveillance. The problems of transparency and trust remain to be solved. The project partners would like to be able to make public when the crime prevention function is active without themselves becoming targets of legal accusations (due to disclosing information related to an ongoing investigation), but this remains unclear.