Report Digital Privacy, Wiv & NGOs event

pro bono connect

Pro Bono Connect
De Wittenstraat 25
1052 AK Amsterdam
The Netherlands

+31 (0) 20 240 29 56
info@probonoconnect.nl

Abstract

Pro Bono Connect (a project of the Dutch section of the International Commission of Jurists) and **TrustLaw** (the legal pro bono service of the Thomson Reuters Foundation) organised an event on the new Intelligence and Security Services Act (the 'Wiv'), which was hosted by **De Brauw Blackstone Westbroek**. The implications of the Wiv for the work of NGOs, lawyers and journalists were discussed by an expert panel in three different discussion rounds. The topics addressed were: 1) untargeted interception, 2) sharing unevaluated data with foreign services, and 3) professional secrecy. The audience was actively involved and they brought forward specific questions and issues.

Terminology

Intelligence services	Inlichtingen- en Veiligheidsdiensten
(Un)targeted interception	(On)gerichte interceptie
Case specific interception	Onderzoeksopdrachtgerichte interceptie
Safeguards	Waarborgen
Review committee on use of powers (TIB)	Toetsingscommissie Inzet Bevoegdheden (TIB)
Supervision commission security and intelligence services (CTIVD)	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensen (CTIVD)
Unevaluated data	Ongeëvalueerde gegevens
Bulk interception	Massa interceptie
Attorney-client privilege	Beroepsgeheim van advocaten
Source protection	Bronbescherming

Introduction

We use digital communication more frequently every day. Personal data, sensitive information and private correspondence: everything is digital. But what about our right to digital privacy? Due to the new Intelligence and Security Services Act 2017 (hereinafter: Wiv) the General Intelligence and Security Service of the Netherlands (AIVD, hereinafter: intelligence service) gets additional competences for data collection. During the event, the implications of the new Wiv on the work of NGOs, lawyers and journalists were discussed.

Doutje Lettinga introduced herself as the moderator of the evening, and gave the disclaimer that she works as a senior policy officer Security and Human Rights at Amnesty International. Although this is an organisation that campaigns against the Wiv, during this event she will be a neutral moderator.

Afterwards she introduced the members of the expert panel:
- **Axel Arnbak**: Lawyer at De Brauw Blackstone Westbroek specialised in digital privacy and communication, affiliate researcher at the Institute for Information Law (IViR).
- **Sarah Eskens**: PhD-candidate at the Institute for Information Law (IViR).
- **Lotte Houwing**: Responsible for the Wiv file at the Public Interest Litigation Project (PILP-NJCM).
- **Jelle Klaas:** Litigation director at the Public Interest Litigation Project (PILP-NJCM).
- **David Korteweg:** Researcher at Bits of Freedom. Currently working on topics such as the intelligence services and reform of European privacy legislation. Previously a lawyer specialised in IT and privacy law.

During three rounds the expert panel discussed three different topics concerning the new Wiv. The executive summary can be found from page 7 onwards.

Round 1 – Unfocused interception

In the first round the expert panel discussed unfocused interception and how this potentially affects the work of NGOs. Central topics were: what are the risks of unfocused interception for NGOs and what are the safeguards to mitigate these risks. These questions were addressed in light of the ability to have real-time access to databases of informants, and the collection of data through databases of third parties.

David started off by pointing out that case specific interception is referred to by the government as 'OOG' which stands for o*nderzoeksopdrachtgerichte interceptie ('oog' in Dutch also means 'eye')*. He continued by introducing the new competences of the intelligence services. In the Wiv of 2002, wiretapping was limited to cable communication of specified targets. In the new Wiv 2017 the scope of data collection is extended to an undetermined amount of people and connections. The issue with the new competences is that they are formulated too broadly and vague. It is currently hard to pinpoint where the power starts or ends. In order to determine what is possible under the new Wiv we can examine the examples given in Parliament. In first instance the (former) Minister stated that it would be possible to collect communication via all WIFI hotspots of a certain city or to wiretap communication from a whole city via a chat service. The government has recently provided different examples such as: collecting information to identify possible terrorists, and identifying cyber-attacks as they happen. They argue that in order to do so, they need to use the new competences which allow them to look at a whole network. The problem with these research assignments is that they have been shown to be very broad. An example of a research assignment could be to monitor all people coming back from Syria.

For David and his organisation this is a major problem. The large amount of data collection the new Wiv allows for is problematic in their opinion, as this inevitably leads to the collection of data of innocent citizens. In a liberal society, like the Netherlands, innocent citizens should not be a target of this kind of interception by the intelligence services. David mentioned that if people are aware they are being observed, they will act differently. He concluded that if this is what the new Wiv does to people, it is at odds with our liberal society and might block social innovation.

Doutje asked Lotte whether she thinks that the fact that people know that their data might be intercepted, will influence their work for an NGO. Lotte answered that she asked her friends, activists and colleagues: 'Are you ever behind your laptop and you find yourself hesitating to google something because someone else might find out?' All said that they were affected by this idea of someone looking over their shoulder, and that it might lead to self-censoring. Although some people might be able to protect themselves using encryption, for many others this is not a realistic or even feasible option. Additionally, she mentioned that NGOs conduct research and publish articles about important topics, but they might not reach the same audience anymore because people could abstain from searching for it online, aware of the fact they can be observed. Similarly, information might be shared less because people will think twice before sharing something controversial. Altogether this would decrease the outreach of NGOs.

Sarah played the devil's advocate for a moment by pointing out that self-censoring or what is sometimes referred to as the 'chilling effect' may barely take place in practice. Studies on this effect have shown that there is a big difference between what people think they will do, and what people actually do. After a while, people tend to forget their concerns of being monitored, and as a result they will not actively censor themselves anymore. Sarah nuanced that this might of course be different if you look at specific

pro bono connect

Pro Bono Connect
De Wittenstraat 25
1052 AK Amsterdam
The Netherlands

+31 (0) 20 240 29 56
info@probonoconnect.nl

groups. Studies were not performed on an NGO target group. In response, Jelle asked how this study was performed. He wondered how one studies something that is not happening, as is the case with self-censoring. You would be looking for something people are actively abstaining from. Sarah emphasized that that is exactly what the studies she referred to showed: people start using the internet in the same way as they did before, as time passes by.

From the audience a remark followed that self-censorship is very much context dependent. If you live in a society where there are no consequences related to what you look up online, as is the case in the Netherlands, the chilling effect might indeed not have a great influence. However, if you live in a country where you might end up in jail or worse, the results of those studies cannot be generalized to such a context. Another remark made by the audience, was that people might be less inclined to contact an NGO, because they are afraid that the organisation's data is being intercepted. Some of the expert panel agreed with this notion.

Axel remarked that many people currently trust the government and the intelligence services. However, we do not know yet who we are trusting. According to him the law needs to balance security and surveillance, in the hypothetical situation where you cannot trust the intelligence services anymore. The dragnet / untargeted interception could in that light be considered as a nuclear option, as it is the most drastic measure available. Axel cannot think of a more dramatic measure that influences so many people at the same time. If there is an apparent reason to use this option there should at least be empirical evidence to support it. Even then, there must be a balance between supervision and very precise legislation.

Doutje raised the point made by the intelligence services, stating that they will throw away 98% of the data they collect, as they are not interested in innocent citizens. She addressed the panel with the question whether this is a reassuring and sufficient safeguard.

David argued that this percentage does not mean much. It depends on what data is collected in the first place. Two percent of a lot of data can still be a very significant amount. In addition, the intelligence services are mainly interested in metadata. This is information about data itself, for example specific details on your communication or the websites you visit. Metadata does not amount to a lot of the online traffic but is still very important and sometimes says more than the actual content of communication. The 98% of your traffic online is what you watch on Netflix, in which they are indeed not interested. The percentage is meaningless, David concludes. Sarah stressed the overall importance of metadata and the value of it, as it concerns data on your behaviour rather than the content of the interaction.

Finally, the independence of the Review committee on use of powers (TIB) was discussed. This committee needs to evaluate the use of competences by the intelligence services.

Sarah explained that the TIB is appointed by a parliamentary procedure, which is independent of the Minister. They are, however, paid by the Minister. Two of the three members need to be former judges, because former judges are expected to have experience with independent thought. The third member needs to be a technical expert. Some safeguards for their independence are the amount of years they are appointed for, and the procedure of firing them.

Axel addressed the point that there has been a lot of critique on the appointment procedure of the current TIB. The procedure demands that the ministry provides three candidates for each position. In the most recent procedure there were only two candidates for the technical position. Eventually, a former intelligence service member was appointed for this position, who campaigns in favour of the

pro bono connect

Pro Bono Connect
De Wittenstraat 25
1052 AK Amsterdam
The Netherlands

+31 (0) 20 240 29 56
info@probonoconnect.nl

Wiv. His expertise and knowledge are impressive but, according to Axel, he cannot be considered independent.

Lotte raised a final issue in this round. She gave an example of an apparent issue the Wiv has and for which no answer yet exists. She described a situation in which the TIB rules an action to be unlawful, however the Minister uses its discretionary powers to approve the interception. In this imaginable scenario it is unclear how far the discretionary powers of the minister go against a negative ruling of the oversight committee, especially as the Minister carries the general responsibility towards the Parliament.

Round 2 – Sharing data with foreign intelligence services

In the second round the sharing of data with foreign intelligence services was discussed, in particular the sharing of unevaluated data, which also contains data of non-targets.

David explained that there is no international agreement on cooperation between foreign intelligence services. The exchange of data governs on the basis of reciprocity (quid pro quo). Consequently it is based on trust, and the problem is that you do not know their hidden agenda.

Sarah emphasises that everybody seems opposed to this part of the Wiv, even the proponents.

Jelle addressed the risks for foreign human rights defenders (HRDs), while cooperating with Dutch partners and NGOs. He gave an example of HRDs from [country X], who themselves were very aware of the risks they are exposed to when they visited Jelle's office. Although they manage to secure themselves accordingly, Dutch counterparts might not be as aware or careful with their data. This is something that we should become more aware of, especially with the new Wiv entering into force. Sharing of unevaluated data increases the risk of sensitive information ending up in the wrong hands. Although information can only be shared in the context of protecting national security, this is quite a vague term as pointed out by Sarah.

From the audience, a question was raised by an NGO whether in the decision to share information with [*country Y*], the economic relationship between the Netherlands and [country Y] can play a role. David responded that it is not so much about the economic relation between the countries, but rather the relationship between the intelligence services. [country Y] unfortunately put this specific NGO on their black list due to their work, which focuses on documenting the systematic violations of human rights within [*country Y*]. For this reason it does not seem like a desirable choice to share the NGO's data with their intelligence services. Sarah responded that the internal situation of a country should be evaluated on the basis of five criteria before sharing data, including the question of respect for human rights in the country concerned.

Another question was raised on whether foreign intelligence services can specifically request interception by the Dutch intelligence services. In response David said this would be possible, however the Dutch intelligence services will determine whether it does not interfere with their normal tasks. This was backed up by Axel who referred to article 89 of the Wiv. Lotte pointed out that the intelligence services are also allowed to provide technical assistance to their foreign counterparts.

One of the last questions in this round concerned the relation between the new Wiv and the General Data Protection Regulation (GDPR). David explained that the GDPR does not apply to the intelligence services, as everything regarding national security falls outside of the scope of the European Union's competences.

pro bono connect

Pro Bono Connect
De Wittenstraat 25
1052 AK Amsterdam
The Netherlands

+31 (0) 20 240 29 56
info@probonoconnect.nl

The final aspect covered in this round was the ability to request real-time access to databases, in which also private companies can be involved. Axel commented that intelligence services can ask for voluntary compliance of employees to grant access to databases without having to inform anyone else in the organisation of this access.

Finally, Jelle expressed the intention of the Public Interest Litigation Project (PILP) to commence a strategic procedure against the Wiv. He said that they will give the government some time after the referendum to implement changes, and explained that litigation is one of the tools to demand adjustments of the law. He emphasised that their goal is to adjust the law, as they do agree that a new law on this topic is needed, since the Wiv 2002 is outdated.

Round 3 – Professional secrecy

In the third and final round professional secrecy of lawyers and journalist was discussed. The discussion focussed on attorney-client privilege for lawyers, and on source protection for journalists.

The consensus was that lawyers have more safeguards regarding professional secrecy under the new Wiv than journalists.

Sarah stated that the safeguards for lawyers are:

1. If the intelligence services want to intercept communication between a lawyer and a client, they need approval from the court.
2. If this data is intercepted accidently, the intelligence service needs to delete it immediately. If they want to use it, they will have to ask the court for permission.
3. The information can only be shared with the public prosecutor's office upon approval from the court.

Only if the intelligence services want to target a journalist and its source and there is a risk of information about the identity of the source being intercepted, they need to specifically request permission of the court. In other cases this is not required. The content of the communication between a source and journalist is not protected by this safeguard (as is the case with communication between lawyers and clients), only the identity of the source is. Unfortunately, NGOs are not explicitly mentioned in or protected under the Wiv.

From the audience a question was raised on whether metadata as such is protected by the new Wiv. The answer was no. Someone suggested that this might be less relevant to protect. Jelle countered this conception by pointing out that it is important to protect information on who you meet, where you meet, for how long, etc. A remark was added from the audience that supported this point by arguing that this is also context dependent. Who you meet could have serious consequences in certain parts of the world. This data could indeed be relevant, for example knowing who seeks help from a lawyer might be sensitive information in itself. Moreover, the intelligence services have direct access to metadata collected by administrative bodies, for example the registration of number plates is included in this data.

Lotte explained that the vagueness of the new Wiv makes it hard to prepare for it or take measures in order to limit its impact on your work. Journalists, lawyers and NGOs are advised to use encryption tools and to be aware of the problems discussed during the event. Axel then commented on the function of vagueness. The Wiv is vague on purpose because, as has been revealed in the past, it serves the intelligence services. Edward Snowden revealed how the intelligence services of the United States use the vagueness of legislation to cross the limits of what is acceptable.

pro bono connect

Pro Bono Connect
De Wittenstraat 25
1052 AK Amsterdam
The Netherlands

+31 (0) 20 240 29 56
info@probonoconnect.nl

Doutje thanked all the members of the panel and the audience and welcomed them for drinks sponsored by the NJCM. Thank you for your participation and interest.

For questions and remarks please contact: info@probonoconnect.nl or www.probonoconnect.nl

pro bono connect

Pro Bono Connect
De Wittenstraat 25
1052 AK Amsterdam
The Netherlands

+31 (0) 20 240 29 56
info@probonoconnect.nl

Executive summary

Round 1 – Unfocused interception

- The scope of data collection is extended to an undetermined amount of people and connections in the new Wiv.
- New competences formulated too broad and vague.
- Data from innocent citizens is inevitably collected.
- Self-censoring or what is called the 'chilling effect' is also problematic for NGOs, as this decreases their outreach.
- Studies might show minor chilling effect in Dutch context, but are likely to have a greater impact in contexts where there are consequences for someone's online behaviour.
- Legislation should be drafted in a way that accounts for the situation where we cannot trust the intelligence services.
- Untargeted interception is the most drastic measure.
- Review committee on use of powers (TIB) has safeguards for independence of its members, such as: the parliamentary appointment procedure and term limits.
- Appointment procedure of current TIB criticized because the procedure was not respected.
- The weight of the Minister's discretionary powers versus a binding decision of TIB is uncertain.

Round 2 – Sharing data with foreign intelligence services

- Sharing between intelligence services based on the principle of reciprocity.
- Large amount of people against the sharing of unevaluated data with foreign intelligence services.
- Awareness of this power is necessary amongst Dutch NGOs dealing with other people's sensitive information, for example foreign HRDs.
- Information can be shared with foreign intelligence services in context of national security. What is considered to be in the interest of national security remains vague.
- For the sharing of data the relation between the intelligence services is more important than the political or economic relations between the countries.
- The intelligence services can grant foreign requests for interception if it does not conflict with the normal tasks of the service. Technical assistance to foreign intelligence services is also allowed.
- The GDPR does not apply to the intelligence services.
- Real-time access to a database can be requested on a voluntary basis to anyone.
- PILP is planning legal proceedings against the Wiv if the government does not improve the law after the referendum.

Round 3 – Professional secrecy

- Lawyers receive greater protection against intrusions on their attorney client privilege than journalist for the protection of their sources.
- The intelligence service needs to request court approval before:
  - intercepting communication between a lawyer and client;
  - if they want to use accidentally intercepted communication between a lawyer and client;
  - if they want to share communication between a lawyer and client with the public prosecutor.
- The intelligence service only needs to request court approval before they are intercepting communication between a journalist and the source if there is a risk of collecting information on the source's identity.
- Vagueness of the Wiv makes it hard to prepare against it. The vagueness also has a function in the way it allows the intelligence services to operate more easily.

pro bono connect

Pro Bono Connect
De Wittenstraat 25
1052 AK Amsterdam
The Netherlands

+31 (0) 20 240 29 56
info@probonoconnect.nl