Privacy International
62 Britton Street
Clerkenwell EC1M 5UY
United Kingdom

Uploaded at: https://www.internetconsultatie.nl/wiv/reageren/1

27 August 2015

Dear Sir/Madam,

RE: SUBMISSION TO THE INQUIRY INTO THE DRAFT LAW ON INTELLIGENCE AND SECURITY SERVICES 2015

We make this submission on behalf of the British human rights organisation Privacy International.

Privacy International was founded in 1990, and is the leading non-governmental organisation promoting the right to privacy across the world. It focuses, in particular, on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation of Economic Co-operation and Development and the United Nations.

Privacy International is actively engaged in scrutinising and critiquing surveillance and signals intelligence laws and policies across the globe. In particular, we are highly active in the ongoing surveillance reform debate in the United Kingdom, where the government will soon seek to enact legislation that will replace all surveillance laws currently in force in Britain. Our internal expertise on surveillance laws and policies is unsurpassed in Britain, where ware also the leading organisation challenging unlawful surveillance practices in British courts.

We wish to express a number of concerns about provisions currently contained in the Draft Law on Intelligence and Security Services 2015 ("the Draft Law"). In particular, the provisions relating to bulk interception, the lack of judicial authorisation, the breaking of encryption, and the hacking of computers and devices raise serious concerns when considering he law's compliance with internationally-agreed human rights norms. We urge the Dutch government to refrain from expanding the Netherland's surveillance powers beyond what is necessary and proportionate in a democratic society. If enacted, not only would this Law make the Netherlands a country with some of the broadest and most intrusive surveillance systems in the world, but it would set a worrying example for countries which don't enjoy your strong democratic

tradition and rule of law.

Below we have set out some of our concerns with the legislation.

Bulk interception powers

We understand that current Dutch law allows for the bulk (i.e. non-specific or non-targeted) interception of ether-bound, but not cable bound, communications where they have a foreign source or destination, for the purpose of signals intelligence ("SIGINT") search. SIGINT selection could be undertaken on any ether-bound communications. However, given that the percentage of domestic communications likely to travel by the ether is negligible, these powers ostensibly allowed only for the bulk interception and analsyis of foreign communications, and even then only ether-bound communications, which in the digital era remains a small percentage of civilian communications. In short, the currently law constrains the ability of the intelligence and security services to do mass surveillance on ordinary individuals' communications, whether they be in the Netherlands or abroad.

The proposed changes will alter this situation severely, essentially introducing a mass surveillance capability into Dutch law. The provisions in the Draft Law relating to non-specific interception do not restrict the exercise of such powers to foreign communication, nor – more importantly – do they restrict interception to ether-bound communications. The result is that the Draft Law authorises the intelligence and security services to conduct mass surveillance of cable bound communications – the cables that carry the private and intimate communications of millions of ordinary people.

The fact that the Draft Law introduces numerous checks and authorisations stages, and requires the interception to be "purpose-oriented" (doelgerichtheid) does not change that the Draft Law will authorise the interception of millions of communications under broad justifications. The Draft Law does not restrict how broad the purpose can be, nor does it restrict how many communications can be intercepted at any one time for the achievement of that purpose. In that context, and assuming that a purpose as broad as "countering terrorism" would be sufficient under the Draft Law (there being no contraindication expressed), the Draft Law does not restrain the intelligence and security services from intercepting all of the communications in the Netherlands all of the time. Furthermore, the Draft Law proposes to extend the retention period for raw intercepts from one year to three, and enables the Dutch intelligence and security services to share raw bulk intercepts (metadata and content) with foreign intelligence and security services.

The interception of communications constitutes an interference with the right to privacy of those communications under Article 8(1), whether made via email, phone, text message, or social media: see e.g. Klass v Germany, 6 September 1978, Series A No 28 at §41; Weber and Saravia v Germany, ECHR 2006 XI at §77; Kennedy v United Kingdom 26839/05 18 May 2010 at §118. The same is true in respect of accessing communications data or 'metadata': see e.g. Malone v United Kingdom 2 Aug 1984, Series A No 82 at §84. Further interferences arise from the collection and retention of such material (see e.g. Amann v Switzerland [GC] ECHR 2000-II – especially on a searchable database – and its transmission to other authorities (Weber and Saravia v Germany at §79)).

The European Court of Human Rights has made no distinction as to the severity of the interception effect when the interception is effected by an automated system or computer. Indeed, the Court has also found that the interception and/or storage of a communication constitutes the interference, and that the subsequent use of the stored information has no bearing on that finding. In Amman v Switzerland (2000) the ECtHR followed its judgment in Leander v Sweden (1987) that "[b]oth the storing and the release of [secret police-register information], which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life...".

Equally, the Court has found that it does not matter whether the information gathered on an individual was sensitive nor whether the applicant had been inconvenienced in any way. In Amman the Swiss government submitted that the establishment of a database of surveillance- derived information was not an interference with the right to privacy because it "contained no sensitive information about the applicant's private life". The Court held (at [70]): "[i]t is sufficient for it to find that data relating to the private life of an individual were stored by a public authority to conclude that... the creation and storing of the impugned card amounted to an interference, within the meaning of Article 8, with the applicant's right to respect for his private life."

In Liberty and Others v United Kingdom the ECtHR reiterated that the mere existence of powers "permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants" (at [57]). This sentiment has been echoed by the United Nations High Commissioner of Human Rights who, in her report on the right to privacy in the digital age, noted that "[t]he very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful."

The Draft Law thus contains a number of provisions which do not comport with international human rights standards. Mass surveillance systems than enable the blanket interception of cable-bound communications, even if for short periods of time, can not be judged to be proportionate. It can never been necessary in a democratic society to place an entire population's communications under the watchful eyes of security services, no matter what ends are served. Moreover, when intercepted communications are shared with foreign intelligence services, not only is a further interference with privacy rights occasioned, but the risk that such data will be subsequent used in a way that further imperils the rights of individuals is increased significantly.

Recommendations:

- **Prohibit the bulk interception of cable-bound communications**
- **Ensure that the Draft Law provides that the interception of communications and acquisition of communications data can only take place on a targeted basis where necessary and proportionate. To this end, ensure the interception powers in the Draft Law meet the standards articulated in the International Principles on the Application of Human Rights to Communications Surveillance (at www.necessaryandproportionate.org)**
- **Ensure that the Draft Law provides equal human rights protections for both**

Dutch citizens and foreigners

Lack of judicial authorisation

It is of serious concern that the Draft Law does not include any role for judicial authorisation, ex ante or ex post. At no stage of the interception process – from collection, to processing, to analysis – is an independent judicial authority consulted for authorisation or review.

If enacted, this element of the Draft Law would make the Netherlands an outlier in terms of best international practice. In order for interferences with the right to privacy, in the form of secret surveillance measures, to be in compliance with Article 8, they must be "in accordance with the law". As explained n Malone v United, the phrase "in accordance with the law" does not merely refer back to the presence of domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention (at [67]).

In Klass, the Court emphasised that "[t]he rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure" (at [55]). Although the Court in Klass agreed that "it is in principle desirable to entrust supervisory control to a judge," it did not go so far as to hold that prior judicial authorisation was required in every case so long as the relevant authorising body was "sufficiently independent" of "the authorities carrying out the surveillance" to "give an objective ruling" and was also vested "with sufficient powers and competence to exercise an effective and continuous control" (at [56]).

There is a growing recognition by courts in Europe and around the world that judicial control of surveillance is the most appropriate and effective safeguard against abuse and guarantor of the lawfulness of surveillance measures. The most recent and pertinent decision comes from the Court of Justice of the European Union ("CJEU") in its decision of Digital Rights Ireland v Minister for Communications & Ors. That case concerned the compatibility of Directive 2006/24/EC of the European Parliament on the retention of communications data, with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ("the Charter") and Article 8 of the Convention. The mandatory blanket retention of data by communications service providers is a surveillance measure justified on the grounds that it is a necessary and effective investigative tool for law enforcement and the protection of national security. The CJEU described the directive as a causing a "wide-ranging" and "particularly serious" interference with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter. In questioning the necessity of the measures mandated by the directive, the Court noted, inter alia (at [62]):

> "In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the

> data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits."

Beyond Europe, courts in Canada and the United States have recently issued decisions affirming that surveillance measures, including access to data retained by communications service providers, must be subject to judicial control or dependent upon the issuance of a judicial warrant. In the case of R v Spencer, the Supreme Court of Canada considered whether police obtaining identity information from an Internet Service Provider (ISP) without prior judicial authorisation, which information was subsequently used to convict an accused of possession of child pornography, was in compliance with the Canadian Charter of Rights. The Court considered that a request from police that an ISP voluntarily disclose identity information amounts to a search. Given that "[a] warrantless search, such as the one that occurred in this case, is presumptively unreasonable" the Crown had to rebut the presumption by establishing that the search was authorised by law, and carried out in a reasonable manner. The Court found that there was no lawful authority for the police's search, and thus it was unlawful.

The US case of Riley v California concerned the search of digital information on a cell phone. The Supreme Court of the United States considered whether police were required by the Fourth Amendment to the US Constitution, which pertains to search and seizure, to obtain a judicial warrant prior to conducting such a search. In a unanimous decision, the Court held that the police generally may not search digital information on a cell phone seized from an individual who has been arrested without first obtaining a judicial warrant.

Recommendations:

- **Provide for ex ante judicial authorisation of interception of communications and acquisition of communications data**
- **Provide for ex post judicial review of surveillance measures**

Powers to break encryption

We are very concerned about Article 33 of the Draft Law, which appears to authorise the intelligence and security services to break or undermine encryption of telecommunications or data, coupled with Article 30-5 to 30-8, which contain the power to compel anyone to assist in the decryption of data by handing over keys or providing decrypted data.

Any attempts to undermine the free use of encryption in digital communications could have serious impacts on the ability of individuals to enjoy their human rights. Encryption is used by every single person who uses a cell phone or a computer, and it protects their personal details and communications from interference by cyber criminals, identity thieves, hackers, and States. The use of encryption is the only way to ensure digital communications – ranging from online financial transactions to cell phone calls to emails – are protected from interference.

By granting the intelligence and security services the power to break encryption, or demand the disclosure of encryption keys, the Draft Law seriously undermines the essential role that encryption plays in modern digital communications. The existence of such a power prevents individuals from being able to reliably communicate knowing that their correspondence is free from interference, and thus has a severe chilling effect on the exercise of free expression. The ramification of such provisions will be felt far beyond the Netherlands: because of the way that digital communications flow across borders and around the world, the existence of targeted powers to remove or defeat encryption in one State has implications for all individuals, and creates a chilling effect for people around the world that is far greater than the sum of isolated instances in which such powers might be deployed.

Furthermore, decryption orders require a delicate assessment of the balance between different human rights (e.g. right to privacy, right to freedom of expression anonymously) and legitimate interests. Such assessment should be made by impartial and independent judicial authorities to effectively guarantee the respect and protection of the right to privacy. This is particularly so in light of the fact that failure to comply with such orders is often considered a criminal offence. Unfortunately, the Draft Law contains no such requirement that a decryption order be judicially authorised.

Recommendations

- **Remove provisions in the Draft Law enabling the security services to break encryption and compel the disclosure of encryption keys**
- **With respect to decryption orders, ensure that the use of such powers is subject to ex ante judicial authorisation**

Expansion of hacking/computer network exploitation powers

Hacking, also known as computer network exploitation (CNE), is an extremely intrusive form of surveillance. It can yield information sufficient to build a total profile of a person, from his daily movements to his most intimate thoughts.

The Netherlands is one of the only countries in the world with legislation permitting its intelligence and security services to use CNE as a form of surveillance. This is because, in most States, hacking is seen as a hugely invasive form of surveillance that may not, in fact, be acceptable in a democratic society. In this context, the provisions in the Draft Law which purport to expand the powers of the services to hack are extremely worrying, both in the sense that they expand already concerning powers, as for the potentially detrimental example they set to other States.

We urge the Dutch government to proceed with caution when expanding the services hacking powers, particularly – as is proposed in Article 30 – introducing greater powers to use CNE for reconnaissance and against third parties.

Such powers are not only extremely intrusive, they also have the potential to undermine the security of the target device and the internet as a whole. Fundamentally, malware and other CNE methods are designed to allow an unauthorised person to control another's computer. The security hole created can be exploited by anyone with the

relevant technical expertise. Passwords, encryption keys and personal files can be collected and copied, either to further other intelligence aims or for a criminal purpose, depending on who has found the vulnerability in the target's system. CNE is the modern equivalent of breaking into a residence, and leaving the locks broken or damaged afterwards.

Furthermore, computer systems are complex and unpredictable. And malware is often not fully vetted to determine its effects on the system.[1] Its installation alone may cause damage, such as the destruction of property or data on the computer, including draft documents or family photos. Intentional alteration is also possible, raising serious concerns regarding the integrity of evidence obtained from the target device. Covert modifications of the system and the planting of data and network logs could lead to misrepresentations of activity and perversions of justice.

The integrity of every network, including the entire internet, is at issue. When the intelligence services release malware, they rarely will be able fully to control its distribution. For instance, the malware the US government used to infect Iranian nuclear facilities, Stuxnet, was later found on computers at the corporation Chevron. [2]If a watering hole is deployed, the government cannot dictate who lands on the infected website. A link to a fake news story, directly emailed to a target, might be forwarded on to others or posted on social media. A server that is the subject of a man in the middle attack could host multiple websites, exposing all those website users to exploitation. If a network communications hub is targeted, that security vulnerability will expose all network users. Or the attack might shut down the network entirely, such as occurred when the US attacked communications infrastructure in Syria.[3] Accordingly, CNE may lead to significant economic losses for network administrators and users and create backdoors for outside access to all personal information contained within the network.

Whether CNE is ever justifiably deployed, therefore, is still an open question. It is very difficult to balance the desire for a new, very powerful surveillance tool with the likelihood of sabotaging the security of our business and personal communications. The privacy intrusion involved further complicates the matter, as CNE reaches further into our lives and thoughts than any heretofore known form of surveillance.

For these reasons, Privacy International urges the Dutch government to very seriously consider if CNE can ever be safely and proportionately used. As the UN Special Rapporteur on freedom of expression has declared, "[f]rom a human rights perspective, the use of such technologies is extremely disturbing."[4]

---

1 Chaos Computer Club, "Chaos Computer Club analyzes government malware" (October 8, 2011), available at: https://www.ccc.de/en/updates/2011/staatstrojaner

2 Rachel King, "Stuxnet Infected Chevron's IT Network," *Wall St. J.* (8 November 2012), available at http://blogs.wsj.com/cio/2012/11/08/stuxnet- infected-chevrons-it-network/.

3 Spencer Ackerman, "Snowden: NSA accidentally caused Syria's Internet blackout in 2012," *The Guardian* (August 13, 2014), available at: http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria- internet- outage-civil-war

4 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, UN General Assembly, A/HRC/23/40, at paragraph 62, available at

Recommendations

- **Assess whether CNE can be used at all in a manner that is necessary and proportionate.**
- **If the CNE power is to be retained, it should only be deployed in the most compelling and narrowly-defined circumstances, with the greatest oversight and safeguards. The following set of principles, if adopted, would help ensure that CNE is used only infrequently when most needed and justified.**
    1. **A CNE operation shall not be undertaken unless there is a high degree of probability that a serious crime or specific threat to national security has been or will be carried out;**
    2. **A warrant for CNE shall not issue unless there is a high degree of probability that evidence relevant and material to a serious crime or specific threat to national security would be obtained by accessing the equipment identified;**
    3. **Any information accessed via CNE shall be confined to that which is relevant and material to the serious crime or specific threat to national security alleged;**
    4. **Before a warrant for CNE is issued, the applicant must demonstrate that other less invasive techniques have been exhausted or would be futile, such that CNE is the least invasive option;**
    5. **The intelligence and security services should not engage in CNE that is likely to make the device targeted, or communications systems generally, less secure;**
    6. **The use of CNE should be subject to the highest levels of judicial authorisation;**
    7. **CNE should be subject to stringent independent oversight;**
    8. **CNE should not be used to circumvent other legal mechanisms for obtaining information;**
    9. **Any information obtained via CNE should be accessed only by authorised intelligence and security agencies, and used only for the purpose and duration for which authorisation was given; and**
    10. **Any individual or entity that has been a target of CNE should be able to seek redress, including those from other countries who may have been targeted.**

---

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf