Response to draft bill Intelligence and Security Services (WiV)

This response is in reaction to the call for contributions for the consultation of the draft proposal of law from the Ministry of Security and Justice (the so called ‘Wet op de Inlichtingen- en Veiligheidsdiensten). We welcome the opportunity to react to the draft legislation. Google will address three elements:

1. General concerns
2. Specific measures regarding encryption and entering communication services
3. Concerns on oversight and transparency

For the purposes of this consultation we will focus on these elements. We shall follow developments closely and reserve the right to raise other issues should these come to the fore.

1. General concerns

The draft bill Intelligence and Security Services (WiV) raises concerns as regards to precedent and international consequences. In part these echo the concerns stated for the draft bill versterkingen bestrijding Computercriminaliteit III.

While we understand the intention of the Dutch Government to ensure an adequate remit for the national security services this bill raises serious issues. The measures proposed are extremely intrusive and detrimental to the fundamental rights of civilians and companies worldwide (privacy, confidentiality of correspondence, freedom of expression, freedom of information, freedom to conduct a business, integrity of property). Clear boundaries, procedural safeguards and strong, independent oversight are essential.

- ○ **Bad global precedent:** First of all the broad range of the draft proposal for example the opening of the possibility to enter communication services and to force de-encryption undermine the trust and safety of the same services. These services, often global by nature, would be compromised and user trust lost. On principle this is setting a bad precedent.

- ○ **Divergence within Dutch Government policy** Secondly undermining the security and trust of these - more often than not - internet based services is in direct contradiction with the intent of the Dutch Government in other area’s. For example establishing the Netherlands as ‘digital gateway’ to Europe.[1] In other areas too it appears to be at odds with international policy ambitions. It contradicts the Dutch leadership on freedom of expression online, and is clearly not an example that one

[1] https://www.rijksoverheid.nl/documenten/rapporten/2013/07/02/strategisch-aanvalsplan-the-netherlands-digital-gateway-to-europe

would want to set for the world.[2] Finally, how would this fit with the chair's statement of the Dutch hosted GCCS 2015?[3]

- **Risk for investment climate:** In 2013 the Netherlands Foreign Investment Agency reported a landmark year for investment. With technology companies leading with a growing investment in for example datacentre investments from 1 to 6 centers and upwards for 500 million euro's.[4] The wider scope of the draft bill would appear to endanger the investment climate in the Netherlands, especially where it concerns these kind of (future infrastructure) investments. The issue of investment climate was also rightly pointed out by Nederland ICT in their consultation on the earlier draft proposal Computercriminaliteit III.[5]

2.Specific measures

This section focusses on two specific measures. The measures are particularly intrusive and detrimental to both user and company trust.

- Paragraph 3.2.2.6 **"Verkennen van en binnendringen in geautomatiseerde werken"**

  This paragraph raises serious concerns. In the paragraph measures mentioned include "entering communication services" and "undoing encryption". The first measure would require a specific request based on a court order. This safeguard is not present as regards to this specific element of the proposal. Also the scope of the article is very broad and opens the possibility to gather metadata (art. 30.9). Also the mention of 'authority to (..) breach any security" (art 30.1) would be very damaging for user and company trust and seriously endanger the safety of worldwide cloud-based systems.

  The article on "undoing encryption (art. 30.5) runs counter long standing efforts on encryption. The vast majority of users benefit from having their data and devices encrypted given the risk of everyday threats like losing a phone or having a computer stolen, account hacking, phishing etc, and governments still have access to user data via valid legal processes.

  Google uses the latest technology to help users stay safe. Encryption is simply the 21st

[2] The Minister of Foreign Affairs published a policy letter focussing on the importance of human rights and freedoms. In the letter internet is specifically addressed as one of the pillars of the human rights policy. In Chapter 2, 'Mensenrechten anno 2013: innovatieve aanpak', the sub-chapter 'Innovatie via internet' states "De wijde verspreiding van internet en mobiele telefoons biedt iedereen de kans om mensenrechten schendingen direct onder de aandacht te brengen. (...) Het potentieel van het internet moet verder worden benut voor mensenrechten.".

[3] https://www.gccs2015.com/news/outcome-conference

[4] https://www.rijksoverheid.nl/actueel/nieuws/2014/03/16/recordaantal-extra-banen-dankzij-buitenlandse-investeringen

[5] Nederland ICT, "Reactie op consultatie Wetsvoorstel Computercriminaliteit III', 1 juli 2013, page 5.

century method of protecting personal documents and communication, just as safes and combination locks were in the past. These new steps protect everyday law-abiding citizens, who may lose their phones, or have them stolen, and therefore be put at risk of identity theft, financial fraud, or worse. Numerous government agencies have encouraged/supported technology companies using encryption.

We have encrypted the private links between our datacenters, some of which are in Europe, and we also encrypt user data in rest. In the most recent versions of Android, encrypting data on the device is the default. In 2015, Google announced that the newest release of the Android mobile operating system will allow for device manufacturers to automatically encrypt data on the device. We're doing this to give consumers more protection; for example, this helps protect the sensitive data that users store on their phones in the event of theft or loss. We have also introduced a Chrome plugin, End-to-End, that enables users to encrypt data before it leaves their browser in such a way that only the intended recipient is able to decrypt it. Most laptop and desktop computers have been protected by encryption for a long time. We believe mobile users should have the same protections.

It's important to note that encryption does not prevent law enforcement from obtaining user data from Google through the legitimate legal channels. In valid emergency situations, we can respond promptly. In other situations, requests for content go through MLAT processes. Furthermore, there are serious doubts surrounding the effectiveness to de-encryption in law enforcement. According to a July 2014 report by the U.S. courts, encryption only foiled investigators in 0.25% of wiretap cases (or 9 out of 3500 cases) in 2013, showing that there are often multiple avenues to the same information if government needs it for a case. Only 41 out of 3500 cases involved any encryption at all, and police were able to circumvent encryption in 32 of those cases.[6]

- Paragraph 3.2.2.7 **“Onderzoek van communicatie”**

  As also mentioned in our contribution to the consultation on the proposal “Wet versterking bestrijding computercriminaliteit III” extraterritoriality is an especially sensitive issue. The entering, breaching or de-encryption of global and/or cloud-based services undermines the security of users and companies worldwide also doing significant damage to the integrity of the systems. So the in article 32.1 (and article 33.1) mentioned option “to tap, receive, record and listen to any form of conversation, telecommunication or information transfer by means of an automated operation, *regardless of where such takes place*” is very worrying.

[6] http://www.uscourts.gov/statistics-reports/wiretap-report-2013#sa9

3. Oversight and transparency

When considering legislation on surveillance we feel strong checks and balances need to be built in. Any oversight needs to be strong, independent and accessible for citizens. In this proposal all these points seems to be lacking. Google supports, with other leading Internet companies, clear principles for global government surveillance reform efforts.[7] Also we would urge the Dutch Government to consider taking into account the standards mentioned in the recent IVIR report 'Ten standards for oversight and transparency of national intelligence services'.

Our users and their trust is a key concern for us. We feel strongly that users need to be informed about what happens to their data when under our care. Our goal is to empower users by providing data to inform discussions about the free flow of information online. That is why we have been publishing a Transparency Report since 2010 and have been continuously working since to broaden the scope of information we publish. Since we issued our first Transparency Report in 2010, government demands for user data have increased by 250% in the U.S. It is simply not the case that US law enforcement agencies using legitimate legal means are either "going dark" or being stymied by Internet companies and their efforts to protect user data using encryption. The current proposal lacks information on how requests and actions by Government would be published for the general public. For our part we will follow our practice in the United States of America to take any requests and actions by the Government into account when publishing our Transparency Report on the Netherlands, also for the security services. We understand that governments have a duty to protect their citizens; it's why we work hard to comply with legitimate legal requests from law enforcement. Between January and June 2014, we provided some or all user data 84% of the time in response to search warrants issued by U.S. law enforcement agencies. Nevertheless, we strongly believe that government surveillance programs should operate under a legal framework that is rule-bound, narrowly tailored, transparent, and subject to complete and independent oversight.

Without transparency and oversight in intelligence and security services, Google can't keep doing what we do best: creating technology that improves people's everyday lives.

Rogier Klimbie, Head of Public Policy Benelux, Google

Email: rklimbie@google.com

[7] http://www.reformgovernmentsurveillance.com/ and http://googlepublicpolicy.blogspot.nl/2015/03/congress-must-reform-our-surveillance.html