LA QUADRATURE DU NET

Surveillance

Following the adoption of the 2013 French "Military Planning Act" (Loi de Programmation Militaire) and Edward Snowden's revelations on the NSA surveillance, La Quadrature du Net developed a series of analysis and proposals regarding the on surveillance exerted carried out by governments on (their) citizens.

What constitutes surveillance encompasses several techniques:

Interceptions of communications (content)

To begin with, one must distinguish judiciary surveillance from administrative surveillance.

The first is regulated by the French Penal Code and carried out whenever a judiciary authority orders it. The latter can be requested by an administrative agent in certain cases (such as preventing terrorism).

The French Surveillance Law of 2015 (Loi Renseignement), the scope of which covers a wide range of techniques such as wire-tapping and listening devices, deals with administrative surveillance carried out mostly by intelligence services.

La Quadrature du Net considers that administrative interceptions of communications:

- should require authorisation from a judiciary judge and be placed under his or her control, during and after the surveillance, or else by an independent body truly able to investigate independently;
- should be challenged before the French Council of State (Conseil d'État) in compliance with the right to a fair trial; in particular through public hearings and disclosure of relevant documents to the claimant. Concerning documents considered "secret-défense" (military/state/top secrets), the French Council of State should have the power to

declassify documents submitted by the administration during the procedure when it considers that their classification is not justified;

- The number of illegal situations and infractions raised by the National Oversight Commission for Intelligence-Gathering Techniques (CNCTR) and the Council of State should be made public. This would prevent a disproportionate extension of the amount of information classified as national security secret.

Storing and analysing connection data

Connection data reveal a huge amount of information on our private life. It is why public authorities (both administrative and judiciary) regularly request access to such data when conducting surveillance operations.

During the hearing on the Priority Preliminary rulings on the issue of constitutionality (Question Prioritaire de Constitutionalité, QPC) about the French Military Programming Act (loi de Programmation Militaire) submitted by La Quadrature du Net, FDN and the Fédération FDN, the rapporteur explained that

«*These changes lead to an exponential growth of the amount of connection data, as well as to an unprecedented improvement of the quality and accuracy of the information, and to a reasonable use [of data] accumulated about a particular person. All this explains the interest of intelligence services*».

We are now facing a situation where « *the fundamental difference between connection data and content data is not as relevant as few years ago. Access to connection data, which is an invasion of privacy, should be reappraised.*».

The legal regime of retention and analysis of connection data should be adapted by taking this new context into account.

The 'Digital Rights' judgement of the European Court of Justice from 8 April 2014, dealing with widespread data retention, leads us to review the applicable national law (articles L. 34-1 et R. 10-13 of the Post and Electronic Communications Code) on this matter/issue.

The principle of generalised data retention is even more questionable since alternative measures of targeted data retention are already in place in about thirty countries. These measures enable investigators to request technical intermediaries to keep specific pieces of data, or to share technical data in their possession. They are efficient and prove that alternatives that respect

fundamental liberties, and are therefore much more proportionate, do exist.

Therefore we must:

- repeal the provisions of article L. 851-1 and following of the CSI (Internal Security Code) introduced by the Surveillance law of 24 July 2015, which fails to define the notion of « information and documents »; // where the notion of "Informations and documents" lacks of defintion
- set up the same type of controls (before, meanwhile and after) to access connection data as to intercept content;
- bring more transparency on the amount of data collected every year from operators and for what reason;
- prohibit devices analysing massive amount of connection data such as the "black boxes" of the article 851-3 of the Surveillance Law of 24 July 2015.

International surveillance and cooperation between agencies

Do supervising authorities know in detail how NSA and DGSI and other intelligence services cooperate?

International surveillance, conducted conducted by the international cooperation of agencies is a way to bypass national legal systems, and can be used for other objectives than the prevention of terrorism. The Campbell report lists several cases in which information gathered by intercepting communications has been used to build economic advantage for a company.

Such interceptions are illegal and illegitimate. They could cause **serious** security problems to our societies: intelligence services are keeping for themselves information on faulty protocols that could be exploited by others (mafia, criminals).

Thus we must:

- protect the universality of rights by setting up the same control regimes when communications are international, and/or collected and analysed abroad. The collection of international communications must only occur after a prior control, and be followed by effective ex-post controls, and should therefore not fall under any derogatory regime.
- to plan independent controls on cooperation agreements with other intelligence agencies in order to ensure that they are not used to bypass national law at the expence of citizen's

privacy.

Defence of the secret of correspondence and improvements to public and private critical infrastructures

In last months we are witnessing a new "crypto war" where the lack of culture about digital issues leads political authorities to distrust and disproportionately repress encryption tools. Encryption fuels fantasies and suspicions of the political class and judges, as shown by this opinion page about encryption, signed by Paris' prosecutor.

However communication encryption is both the expression of the right to anonymity and a necessity to protect oneself, and is encouraged by ANSSI (National Agency for Computer Security) and several European bodies.

La Quadrature du Net calls to:

- promote encryption of communications by requiring from operators and service providers to provide state-of-the-art encryption (typically, Orange (the largest French telecommunication firm) does not provide SSL/TLS for emails).
- a guarantee of the right to encryption and to anonymity online

Citizens taking back control of technology and their personal data

Citizens should be able to protect their data and privacy against generalised surveillance and economic intelligence. For this purpose they should be informed about the consequences of endangering/undermining privacy and be aware of solutions and tools to protect their data. The aim is to give a real decision-making and control power to citizens.

Thus we must:

- encourage the development of free software for decentralised services and end-to-end encryption (that is, that messages sent to a recipient are encrypted locally before being sent over the network) in order to enable users to regain control of their infrastructures. ;
- enable the development of security tools through tax incentive mechanisms and public procurement but also by supporting development programmes and the use of it in higher

education and research.;

- foster the development of trusted hardware, with free designs, especially for mobile communication infrastructures, wifi and routing.