Alain Pannetrat
IT Specialist, Commission Nationale de l'Informatique et des Libertés

Workshop on Botnet Detection, Measurement, Disinfection and Defence

IN THE PRIVACY OF BOTNET COMMUNICATIONS

Disclaimer

The views expressed in this presentation are those of the author and the colleagues that helped him prepare this presentation; they do not represent an official position of the CNIL or of the Article 29 Working Party.

Alain Pannetrat

apannetrat@cnil.fr

Can botnet communications be intercepted, analyzed and/or blocked?

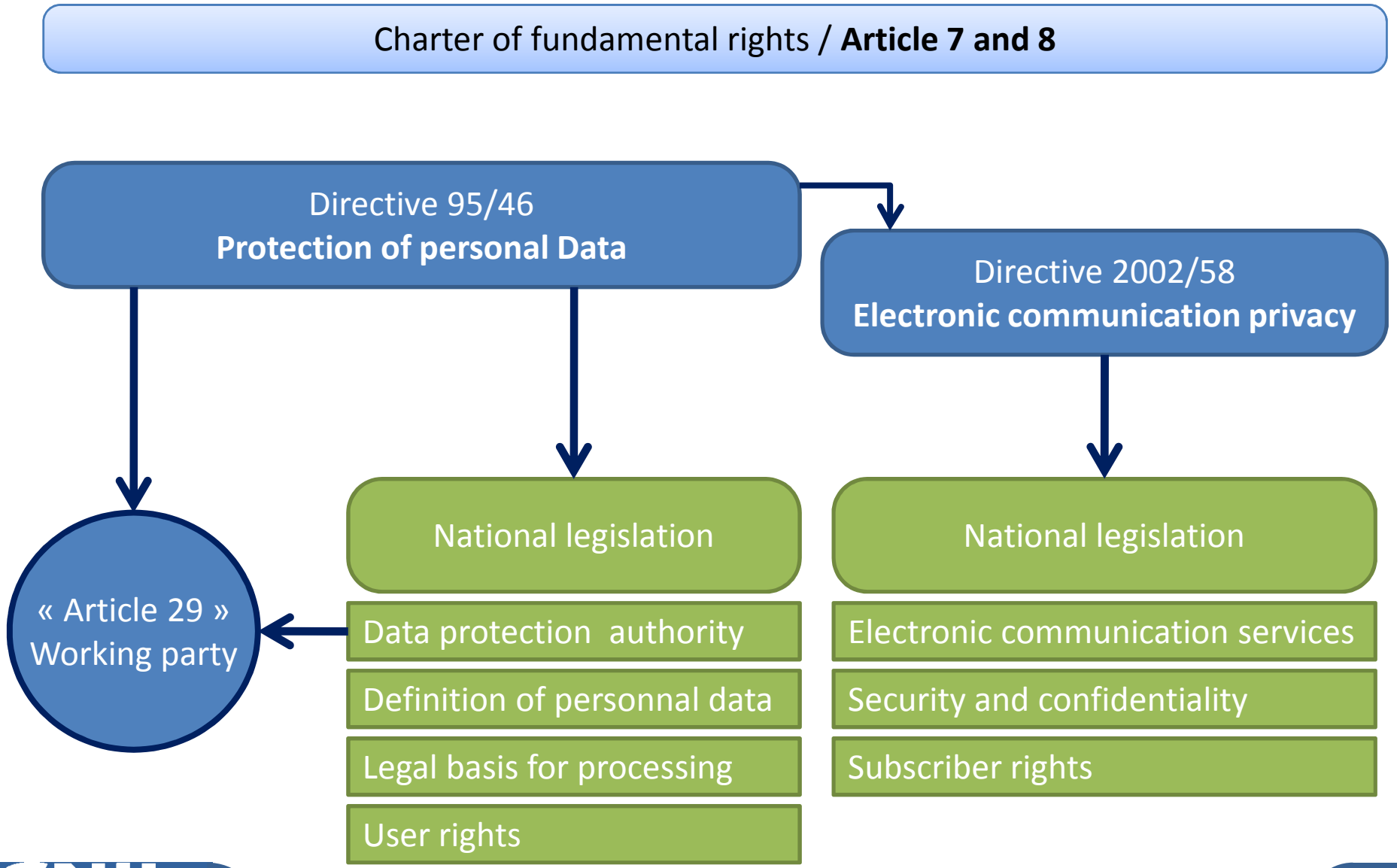
By whom?
Where?

Charter of fundamental rights of the European Union.

- Article 7
  Respect for private and family life
  - Everyone has the right to respect for his or her private and family life, home and communications.

- Article 8
  Protection of personal data
  1. Everyone has the right to the protection of personal data concerning him or her.
  2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
  3. Compliance with these rules shall be subject to control by an independent authority

Legal framework



The balance of directive 2002/58 (mod. in 2009)

ARTICLE 5

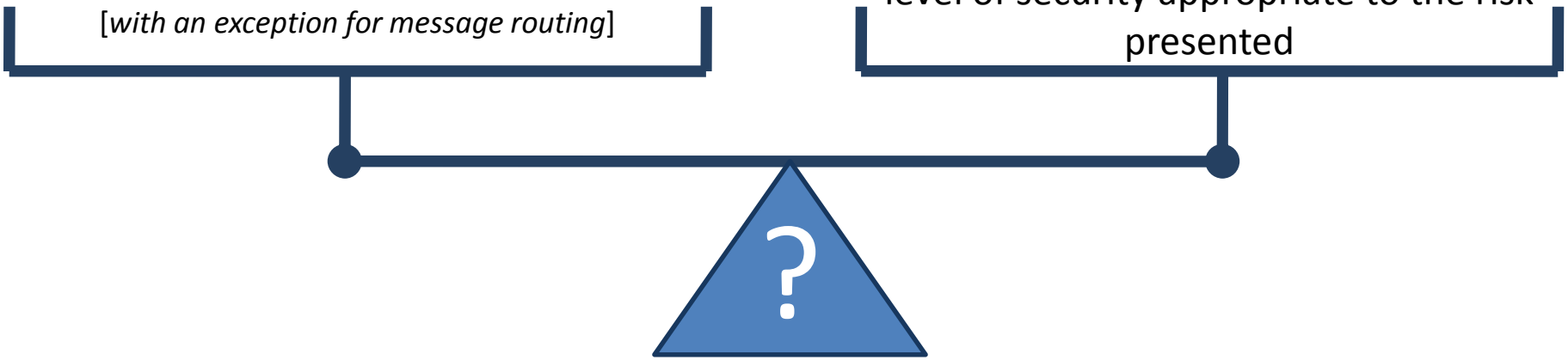
“ Member States shall ensure the **confidentiality** of communications and the related traffic data […]. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so […].

[*with an exception for message routing*]

ARTICLE 4

“ The provider of a publicly available electronic communications service must take appropriate […] measures to safeguard **security** of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. […]

Having regard to the state of the art […], these measures shall ensure a level of security appropriate to the risk presented



Where does the balance stand?

- For *traffic data*, some exceptions to article 5 are explicitly laid down in 2002/58, such as for billing purposes.

- WP29 opinion 2/2006 on email screening for viruses:
  - *"using filters for the purpose of Article 4 can be compatible with Article 5"*.
  - Should be done without prejudice to confidentiality of communications.
  - Seems to suggest that **for the strict purpose of security**, eletronic communication service providers can:
    - Perform **traffic data** analysis
    - Perform **content data** analysis (DPI ?)

This gives ISPs a central role in the fight against botnets

What about other actors?

Traffic data and IT security service providers

Recital 53 of directive 2009/136 (modifying 2002/58):

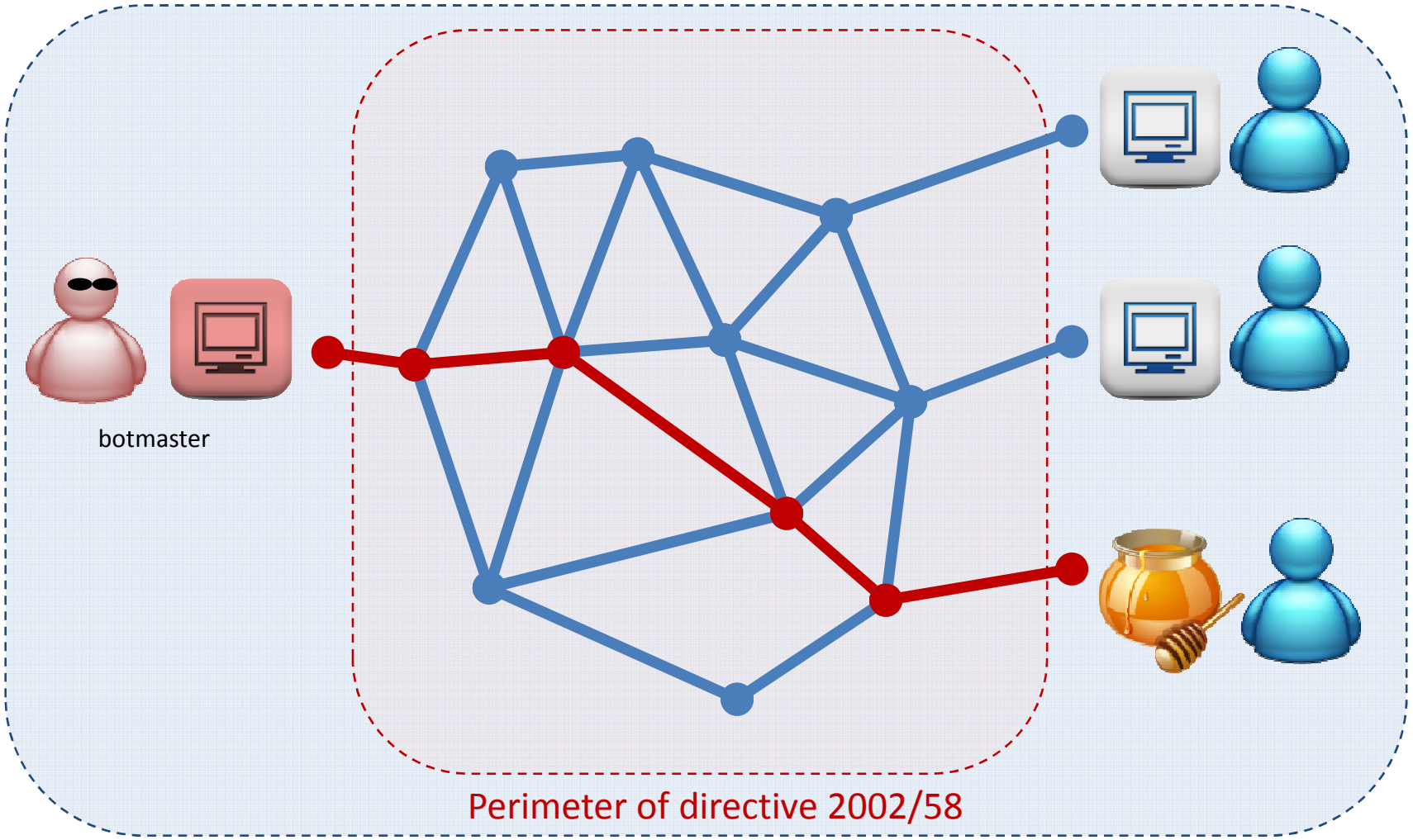
“

The processing of traffic data to the extent strictly necessary for the purposes of ensuring network and information security […] **by providers of security technologies and services** when acting as data controllers is subject to Article 7(f) of Directive 95/46/EC.

“

This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

Honeypots, honeynets and darknets…



Honeypots, honeynets and darknets…

- Article 7(f) of directive 95/46:
  - “processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject […]
- Arguable that “security” is a legitimate interest for:
  - Security service providers
  - Academics specialized in security research
- Honeypots strongly mitigate the risks of interfering with “private” correspondence
  - Interception is unlikely to attack the “fundamental rights” of users.
  - IRC Botnets control commands are unlikely to be “private correspondence”…

Grey areas

- National implementations of Directives add some complexities in some member states:
  - Implementations of directive 2002/58 may put further constraints on the processing of content or traffic data.
    - French legislation explicitly prohibits processing content data by ISPs.
  - Implementations of directive 95/46 may introduce additional legal constraints for some forms of data processing such as:
    - « blacklisting » (IP adresses).
    - Collecting data considered as « related to criminal offences ».

- Deep Packet Inspection has a bad « reputation »:
  - Behavioral adverstising such as « Phorm ».
  - Traffic management issues and net neutrality.

Thank you for your attention