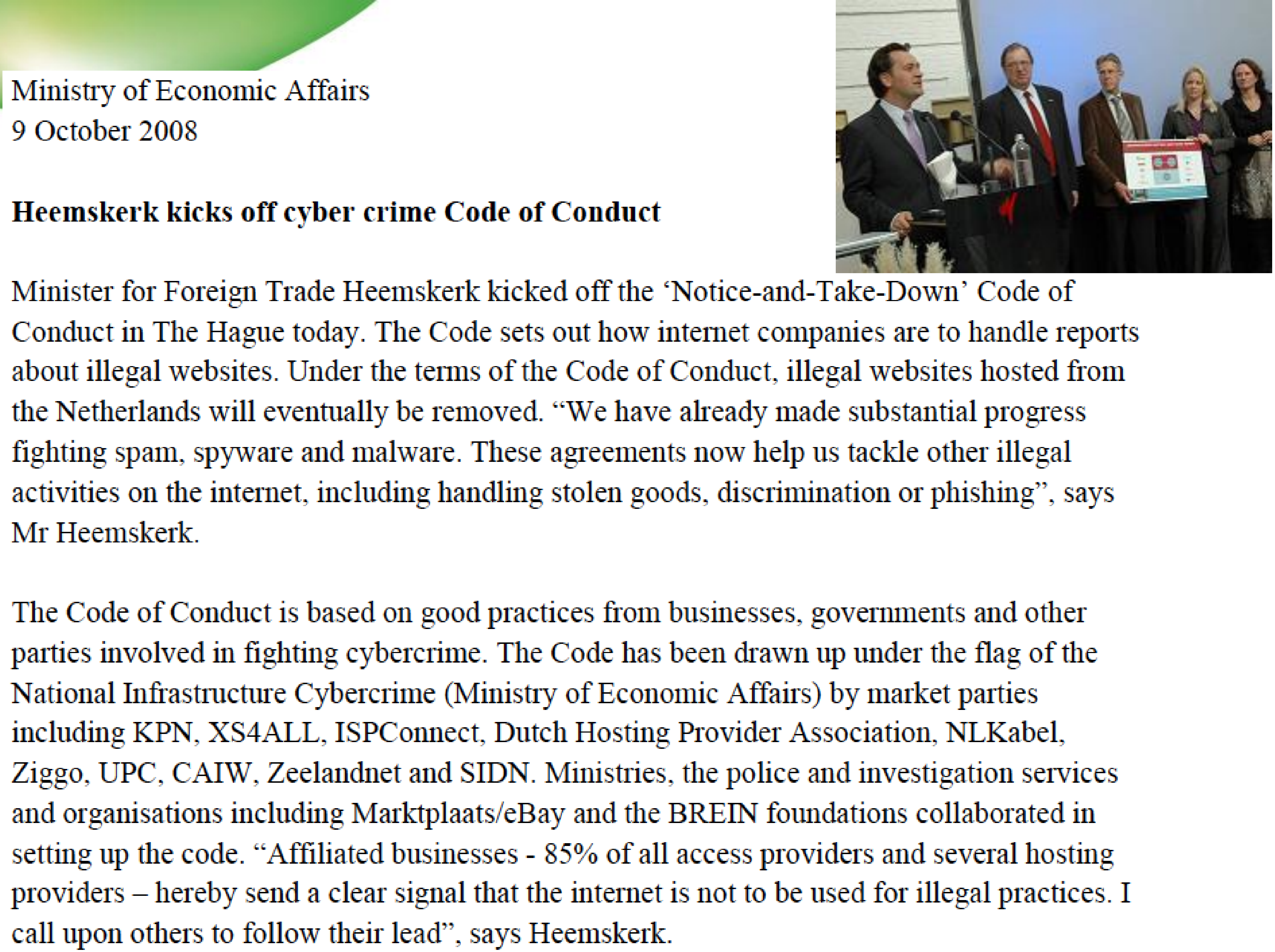
Privacy implications of voluntary exchanges of information

CNSA/LAP Conference, Lisbon

Gert Wabeke
8 October 2009



Ministry of Economic Affairs
9 October 2008

Heemskerk kicks off cyber crime Code of Conduct

Minister for Foreign Trade Heemskerk kicked off the ‘Notice-and-Take-Down’ Code of Conduct in The Hague today. The Code sets out how internet companies are to handle reports about illegal websites. Under the terms of the Code of Conduct, illegal websites hosted from the Netherlands will eventually be removed. “We have already made substantial progress fighting spam, spyware and malware. These agreements now help us tackle other illegal activities on the internet, including handling stolen goods, discrimination or phishing”, says Mr Heemskerk.

The Code of Conduct is based on good practices from businesses, governments and other parties involved in fighting cybercrime. The Code has been drawn up under the flag of the National Infrastructure Cybercrime (Ministry of Economic Affairs) by market parties including KPN, XS4ALL, ISPConnect, Dutch Hosting Provider Association, NLKabel, Ziggo, UPC, CAIW, Zeelandnet and SIDN. Ministries, the police and investigation services and organisations including Marktplaats/eBay and the BREIN foundations collaborated in setting up the code. “Affiliated businesses - 85% of all access providers and several hosting providers – hereby send a clear signal that the internet is not to be used for illegal practices. I call upon others to follow their lead”, says Heemskerk.

De Telegraaf

Friday August 14, 2009, 19:30

Providers initiate action against botnets

The Hague - Fourteen Dutch internet providers take a joint initiative in their fight against botnets. Collectively they have drafted a covenant, stating they will share knowledge and information on this form of cybercrime. The cooperation in its intention should lead to quick response and measures against botnets. This was announced by the providers on Friday.

Information exchange between public and private bodies

- Type of information that can be shared
  - Socially relevant information; i.e. threats, virus alerts (CERT)

- Process of the information exchange between public and private bodies
  - ISP's use process of the trusted complainer (mutual trust model for abuse reporting).
    - peer-to-peer feedback loops between abuse departments of ISP's (ARF) which give indication of spam (based on "this is spam indication")
    - ISP's aim to fight SPAM as direct possible (indication for thrust)
  - Public authority will issue a formal request, based on an assessment of complaints received
    - Information exchange is casus driven

- Role and influence of legislation
  - International harmonization of measures against SPAM
  - Effective enforcement