

Mr Opstelten  
Minister of Security and Justice  
Schedeldoekshaven 100  
2511 EX The Hague

30 November 2012

Re: Dutch plans to remotely conduct searches and delete data on foreign computers

Dear Mr Opstelten,

We would like to express our grave concerns about your plans to grant Dutch police the authority to break into local and foreign computers and remotely conduct searches and delete data in the course of a criminal investigation.

Under your proposal, if the location of a particular computer cannot be determined, the Dutch police could do this without judicial oversight from the country where the device is based. It is even uncertain whether a legal assistance request would be required if the location of the computer is indeed known.

Although your aim to address cybercrime is laudable, the proposal is not an acceptable solution to the problem at hand.

Firstly, these powers, even if only applied domestically, would already seriously restrict the privacy of the suspect and all non-suspects whose data are on the computer which is being accessed. International and European human rights law require any measure restricting such a fundamental right to be necessary in a democratic society and proportionate to the legitimate aim pursued. You have failed to demonstrate the necessity and proportionality of your proposal.

Meanwhile, the proposal poses serious risks to cybersecurity and the global internet. Giving governments the authority to remotely break into computers would create a perverse incentive for them to keep information security weak. As governments would have an interest in keeping vulnerabilities to themselves and exploit them for their own purposes, leaving millions of innocent computer users at risk.

Furthermore, expanding these powers internationally would multiply the already highly problematic nature of your proposal. A measure aimed at breaking the law in the country where a computer is located is by definition arbitrary and therefore illegal under international law. Needless to say, breaking the law to enforce the law in other countries would also violate national sovereignty.

This problem is aggravated by the fact that other countries will in all likelihood follow the initiative of the Netherlands. This will lead to a situation where countries will enforce local laws on foreign computers, instead of investing in international enforcement cooperation.

These local laws would obviously not solely address your definition of cybercrime, but also target political opposition, journalists and dissidents. Attacks against computers for various reasons such as blasphemy, hate speech, homosexuality or copyright infringement are likely.

This is even more pressing since groups such as journalists often use anonymisation services such as Tor to express themselves freely without fear for retaliation. It is precisely these computers that are likely to be targeted without judicial oversight from the country where they are located.

Given the human rights implications and the risks it poses to cybersecurity and the global internet, we strongly urge you to withdraw your proposal.

Yours sincerely,

- April – France
- Access – International
- Agorà Digitale – Italy
- Alternative Informatics Association – Turkey
- Article 19 – UK
- Association for Technology and Internet – Romania
- Bitbureauet – Denmark
- Bits of Freedom – Netherlands
- Bruce Schneier – US
- Chaos Computer Club – Germany
- Civil Rights Society Vrijbit – Netherlands
- Digitalcourage (FoeBuD) – Germany
- Digitale Gesellschaft – Germany
- Digital Rights – Ireland
- Electronic Frontier Finland – Finland
- Electronic Frontier Foundation – International, US
- European Digital Rights (EDRi) – Europe
- Foundation for Information Policy Research (FIPR) – UK
- Free Press Unlimited – Netherlands
- Global Voices – International
- Humanistic Association – Netherlands
- Imaginons un réseau Internet solidaire (IRIS) - France
- International Modern Media Institute (IMMI) – Iceland
- Internet Protection Lab – Netherlands
- Internet Society – Bulgaria
- IT-Political Association of Denmark – Denmark
- Iuridicum Remedium (IuRe) – Czech Republic
- La Quadrature du Net – Europe, France
- Net Users' Rights Protection Association – Belgium
- Netzpolitik – Germany
- No2-ID Foundation – Netherlands
- Open Rights Group – UK
- padeluun – Germany

- Panoptikon Foundation – Poland
- Parents Online – Netherlands
- Platform for the Protection of Civil Rights – Netherlands
- Privacy First Foundation – Netherlands
- Privacy International – UK
- Quintessenz – Austria
- Richard Stallman – US
- Ron Deibert, Director, The Citizen Lab and Canada Centre for Global Security Studies, University of Toronto – Canada
- Statewatch – UK
- The Tor Project – US
- Vrijdschrift / ScriptumLibre – Netherlands