

# CDT Calls for Data Privacy Safeguards in The EU Cybersecurity Directive

by [Jens-Henrik Jeppesen](#) [1]  
June 6, 2013

Another week, another high-profile cyber attack, this time on a popular [Lithuanian news website](#) [2], causing slowdown of that [country's Internet traffic](#) [3]. The challenge of how to deal effectively with cybersecurity threats confronts governments across the globe. This week, NATO defense ministers [met in Brussels](#) [4] to review the state of the alliance's capabilities and readiness to respond to threats to information infrastructures. NATO Secretary General Anders Fogh Rasmussen has named cyber attacks the top threat facing the Alliance's members in the 21st century.

The EU also has identified cybersecurity as a priority, as set out in the Commission's policy programme, the Digital Agenda for Europe. In February 2013, the European Commission unveiled its plans for a common EU cybersecurity strategy. The package is now going to be discussed by the European Parliament and Member States.

The core of the Commission's strategy is a Proposed Directive Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union (the Cybersecurity Directive).

CDT agrees with the Commission's conclusion that cybersecurity requires EU-level action, and we also support the Commission's goals as described in the Directive, but in [our extensive work on cybersecurity](#) [5], we focus on advocating measures that increase the security of Internet communications without compromising human rights or innovation. It is with these principles in mind that CDT [has raised concerns](#) [6] with certain provisions of the Directive.

In particular, we focus in our comments on the question of collection and sharing of cyberthreat information among market operators and governments, which is a major theme in the proposed Directive. Most importantly, CDT would like to see more explicit data minimization safeguards in the text. In the current draft, there seems to be no limit to the types and quantities of data to be collected, stored, and shared by Member State authorities. CDT recommends that the Cybersecurity Directive include a clear and unambiguous definition of the types of data that can be considered relevant for collection and processing for cybersecurity purposes, and clearly stated obligations on authorities to delete and dispose of such data once they are no longer required to manage cybersecurity risks and threats.

The need for data minimization is particularly important because of the very wide range of private sector companies that are subject to the information sharing obligations in the Directive. These would include e-commerce operators, Internet payment gateways, social networks, search engines, cloud computing services, and application stores, but the list is explicitly non-exhaustive - so new types of companies can be added as authorities perceive the need for it.

Cybersecurity is just one of the areas in which government authorities are increasingly seeking systematic access to data held by private sector companies. Governments collect private sector data for a widening range of purposes, often legitimate and reasonable ones such as public safety, tax collection, and law enforcement. However, as the amounts of personal data generated and stored through everyday communications and commercial transactions increase, and as new means become available for government authorities to access these data, often on a systematic, automated basis rather than on specific request involving due process, the risk of misuse of data with serious consequences for the people involved also increases. Cybersecurity is one among many fronts in this debate. The likelihood of growing data collection and sharing for cybersecurity purposes highlights the urgency of developing appropriate data protection rules.

CDT has been engaged in extensive research [in this area](#) [7]. These issues will no doubt continue to rise in importance going forward, and we will continue to focus on them.

The copyright © 2013 by the Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

**Source URL:**

<https://cdt.org/blogs/jens-henrik-jeppesen/0606cdt-calls-data-privacy-safeguards-eu-cybersecurity-directive>

**Links:**

- [1] <https://cdt.org/personnel/jens-henrik-jeppesen>
- [2] <http://www.delfi.lt>
- [3] <http://www.economist.com/blogs/easternapproaches/2013/06/lithuania-under-cyber-attack>
- [4] <http://www.reuters.com/article/2013/05/30/net-us-nato-cybersecurity-idUSBRE94T0Z220130530>
- [5] <https://www.cdt.org/issue/security-surveillance>
- [6] <https://www.cdt.org/files/pdfs/Concerns-European-Commission-Proposal-Cybersecurity.pdf>
- [7] <http://idpl.oxfordjournals.org/content/2/4/195.full>